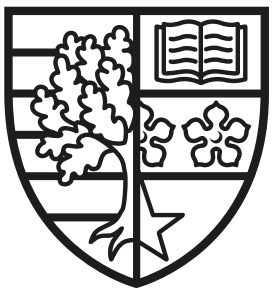
Quantum Information Processing with Photonic Graph States

Massimiliano Proietti

Submitted for the degree of
Doctor of Philosophy

Heriot-Watt University



Department of Physics,
School of Engineering and Physical Sciences.

July, 2020

Abstract

Quantum information processing is the field of science where the underlying principles of quantum mechanics are explored and exploited to achieve a given goal. In quantum information theory, the so-called graph states can be used as a resource to encode, manipulate and read-out quantum information. In the present thesis, graph states are experimentally realised up to six qubits by means of single photons at telecom wavelength. High-quality graph states and high generation rates are achieved. These photonic graph states are then employed in three independent experiments covering the topics of quantum foundations, quantum key distribution, and quantum metrology respectively. The first experiment shows for the first time the incompatibility of quantum mechanics with the notion of "observer independence". The second experiment, demonstrates the use of graph states to distribute a secret and common key among several users. A so-called conference key agreement protocol is demonstrated between four users achieving unprecedented rates at which graph state are distributed over long distances. Finally, the third experiment is proposed to demonstrate the feasibility of phase estimation in realistic noisy environments. Graph states' robustness against noise is enhanced with a novel technique based on experimentally-friendly local encoding. In conclusion, the present thesis provides a comprehensive experimental investigation on the generation and use of graph states for advanced quantum information processing.

To my parents and to the loved ones.

Acknowledgements

First, I would like to thank my supervisor Alessandro. You guided and advised me throughout my Ph.D. experience. You have been always available for unannounced meetings, and I am extremely thankful for that. I enjoyed our discussions, where we could chat about science as well as more general everyday life problems. Then, I should thank my labmates and friends. Francesco, Peter, and Dmytro we shared the lab in the early days, when the optical bench was mostly an empty space. Thanks for the fun we had back then and in particular Francesco, thanks for the countless of discussions we have had from the beginning to the end of my experience, and I enjoyed some italianity sometimes. Alex, I hope you enjoyed your very first tomography, and thanks for all the help when you joined us in the main lab. We had lot of fun during the Wigner (and in the dip). Martin, thanks a lot for your close guidance during my most productive year of the Ph.D. You initiated me in the realm of the foundations of quantum mechanics and in return you received a remarkable number of questions, which you always answered thoroughly. For this I am extremely grateful. Joseph, I am sorry you happened to work with me when I was not as enthusiast about science as I used to be. Although our experiment together took forever (like our discussions), I enjoyed it after all, and mostly because of your contagious enthusiasm for physics. Thanks for that. Chris I am sure we would have had much fun if you had joined us earlier, but you preferred quantum dots to our nice and probabilistic sources. Anyway we had a chance to have a couple of nice chats which I enjoyed. Berke, we shared the office rather than the lab and I should thank you for the bakery you often brought there, it was a nice element of the office. Speaking of which, I must thank Neil as well. When I say "the office", I mean your office. Thanks for all the funny conversations we had, but let me say that I am still waiting for the golf promise you (and Alex) made. Finally, thanks to all my friends in Edinburgh and Glasgow for all the nights out which definitely helped me to forget about science and single photons.

Research Thesis Submission

Please note this form should be bound into the submitted thesis.

Name:	Massimiliano Proietti		
School:	School of Engineering and Physical Sciences		
Version: *(i.e. First, Resubmission, Final)*	First	Degree Sought:	Doctor of Philosophy

Declaration

In accordance with the appropriate regulations I hereby submit my thesis and I declare that:

1. The thesis embodies the results of my own work and has been composed by myself
2. Where appropriate, I have made acknowledgement of the work of others
3. The thesis is the correct version for submission and is the same version as any electronic versions submitted*.
4. My thesis for the award referred to, deposited in the Heriot-Watt University Library, should be made available for loan or photocopying and be available via the Institutional Repository, subject to such conditions as the Librarian may require
5. I understand that as a student of the University I am required to abide by the Regulations of the University and to conform to its discipline.
6. I confirm that the thesis has been verified against plagiarism via an approved plagiarism detection application e.g. Turnitin.

ONLY for submissions including published works

Please note you are only required to complete the Inclusion of Published Works Form (page 2) if your thesis contains published works)

7. Where the thesis contains published outputs under Regulation 6 (9.1.2) or Regulation 43 (9) these are accompanied by a critical review which accurately describes my contribution to the research and, for multi-author outputs, a signed declaration indicating the contribution of each author (complete)
8. Inclusion of published outputs under Regulation 6 (9.1.2) or Regulation 43 (9) shall not constitute plagiarism.

* *Please note that it is the responsibility of the candidate to ensure that the correct version of the thesis is submitted.*

Signature of Candidate:		Date:	08/05/2020

Submission

Submitted By *(name in capitals):*	MASSIMILIANO PROIETTI
Signature of Individual Submitting:	
Date Submitted:	08/05/2020

For Completion in the Student Service Centre (SSC)

Limited Access	Requested	Yes		No		Approved	Yes		No	
E-thesis Submitted ***(mandatory for final theses)***										
Received in the SSC by *(name in capitals):*						Date:				

Inclusion of Published Works

Please note you are only required to complete the Inclusion of Published Works Form if your thesis contains published works under Regulation 6 (9.1.2)

Declaration

This thesis contains one or more multi-author published works. In accordance with Regulation 6 (9.1.2) I hereby declare that the contributions of each author to these publications is as follows:

Citation details	Proietti M, Pickston A, Graffitti F, Barrow P, Kundys D, Branciard C, Ringbauer M, Fedrizzi A. Experimental test of local observer independence. Science advances. 2019 Sep 1;5(9):eaaw9832.
Author 1, Author 2, Author 3, Author 4, Author 5	Performed the experiment and collected the data.
Author 1, Author 3	Analysed the data.
Author 7, Author 8, Author 6	Conceived the project and designed the experiment.
Author 6	Developed the theory results.
Signature:	
Date:	08/05/2020

Citation details	Proietti M, Ringbauer M, Graffitti F, Barrow P, Pickston A, Kundys D, Cavalcanti D, Aolita L, Chaves R, Fedrizzi A. Enhanced multiqubit phase estimation in noisy environments by local encoding. Physical review letters. 2019 Nov 1;123(18):180503.
Author 1, Author 2, Author 3, Author 4, Author 5, Author 6	Characterised the experimental setup.
Author 1, Author 2	Designed and performed the experiment, collected and analysed the data.
Author 10	Conceived the project.
Author 7, Author 8, Author 9	Developed the theory results.
Signature:	
Date:	08/05/2020

Citation details	Proietti M, Ho J, Grasselli F, Barrow P, Malik M, Fedrizzi A. Experimental quantum conference key agreement. arXiv preprint arXiv:2002.01491. 2020 Feb 4.
Author 1, Author 2, Author 4	Designed and performed the experiment.
Author 1, Author 2	Collected and analysed the data.
Author 3	Developed the theory results.

Author 5, Author 6	Conceived the project.
Signature:	
Date:	08/05/2020

Citation details	Graffitti F, Barrow P, Proietti M, Kundys D, Fedrizzi A. Independent high-purity photons created in domain-engineered crystals. Optica. 2018 May 20;5(5):514-7.
Author 1, Author 2, Author 3, Author 4	Designed and performed the experiment, collected and analysed the data.
Author 1	Developed the theory results.
Author 5	Conceived the project.
Signature:	
Date:	08/05/2020

Citation details	Shahandeh F, Ringbauer M, Proietti M, Costa F, Lund AP, Graffitti F, Barrow P, Pickston A, Kundys D, Ralph TC, Fedrizzi A. Assisted Macroscopic Quantumness. arXiv preprint arXiv:1711.10498. 2017 Nov 28.
Author 2, Author 3, Author 6, Author 7, Author 8, Author 9	Designed and performed the experiment, collected and analysed the data.
Author 1, Author 4, Author 5	Developed the theory results.
Author 11, Author 12	Conceived the project.
Signature:	
Date:	08/05/2020

Contents

Chapter 1

Introduction

Like a relay race where runners of the same team independently contribute to reach a common goal, quantum information processing is the result of the interplay between pure theory and experiments. Posing new fundamental questions, leads to advances in the technology required to experimentally test those questions. In turn, the development of new technologies allows new questions to be posed. In this thesis, the bidirectional character of quantum information processing will manifest in three independent experiments. I will start with an experiment related to the topic of quantum foundations, showing the pivotal relationship between observers and measurement outcomes in quantum mechanics. I will then pass to two more technical experiments, demonstrating the feasibility of modern quantum technologies for practical tasks such as the simultaneous sharing of a secret key among multiple parties, and quantum metrology in the presence of noise. The common thread between the three chapters, is the state-of-the-art experimental setup employed for each experiment, that is a photonic platform for multi-qubit graph states.

I introduce the notion of a multi-qubit graph state in Chapter 2 with the help of the so-called stabilizer formalism. Chapter 3 will be a virtual lab tour where I describe the photonic platform in all its features and an exemplary realisation of a graph state will be given. I proceed then with three experiments, in Chapters 4, 5 and 6.

In Chapter 4, I show and experimentally test the incompatibility of the quantum theory with the three assumptions of "freedom-of-choice", "locality" and "observer independence".

In Chapter 5, I use graph states to distribute and share a common and secret key among four users. Here, the photonic platform is connected with long fibres to distant users, reproducing a quantum network..

In Chapter 6, I introduce noise in the platform to simulate realistic scenarios. In such adversary conditions, quantum information processing becomes more problematic and in the chapter I show how simple local encoding can be used to protect against dephasing, which will be useful long before full-scale error correction can be deployed. The efficacy of the method is attested by running a so-called phase estimation protocol in a noisy environment.

Each Chapter is thought to be self-contained with the support of Chapter 2 and Chapter 3 whenever necessary.

In conclusion, in Chapter 7 I give some final remarks and perspective for future research directions.

Chapter 2

The Stabilizer Formalism and Graph States

When moving from the single qubit scenario into the multi-qubit case, a plethora of possible quantum states can be explored. In this Chapter, I introduce the theoretical background underlying the notion of a so-called graph state. A graph is an abstract object where vertices are connected by a set of edges, and in this chapter I will show how this mathematical object can be mapped into a multi-qubit quantum state in turn representing a physical system. As we will see, the direct use of a graph and transformations on it, can tremendously simplify the treatment of a multi-qubit system respect to the canonical approach based on the quantum state formalism. Therefore, since in this thesis multi-qubit states will be a constant presence, understanding the graph states formalism is paramount.

I start in Sec. 2.1 with the so-called stabilizer formalism, which provides the underlying rules to describe any graph state. In particular, the unitary evolution and measurement rules for quantum states are reformulated within the stabilizer formalism in Sec. 2.2 and Sec. 2.3, respectively. We move then to Sec. 2.4 where I describe with the stabilizer formalism how to construct graph states, and in Sec. 2.5 I introduce simple graphical rules equivalent to the unitary evolution and measurements on quantum states. These purely graphical rules are crucial to simplify the description of multi-qubit states. Finally, in Sec. 2.6, I give some more mathematical tools that is, quantum state tomography, state fidelity and entanglement measures, useful to characterise graph states when realised in practice.

2.1 Stabilizer Formalism

The stabilizer formalism is a powerful toolkit in quantum information theory. It was introduced by Gottesman [1] in the context of quantum error correction and lately adopted in problems such as measured-based quantum computation (MBQC) [2, 3] and entanglement detection [4]. In this section, the basic ideas of this formalism are presented, focusing on its application within the graph states framework. For a more rigorous and extended description of the formalism the reader is referred to text books as Refs. [5–7] or papers as Refs. [8, 9].

For N qubits, we can define the so called *Pauli Group* as:

$$\mathcal{P}_N := \{\pm 1, \pm i\} \times \{I, X, Y, Z\}^{\otimes N}. \tag{2.1}$$

Where $\{X, Y, Z\}$ are the 2×2 Pauli matrices $\sigma_x, \sigma_y, \sigma_z$ respectively and I the identity matrix. Given any N-qubit quantum state $|\psi\rangle$ we can select from the Pauli group all the operators S_i such that:

$$\forall S_i \in \mathcal{P}_N, \quad S_i|\psi\rangle = |\psi\rangle. \tag{2.2}$$

In other words, $|\psi\rangle$ is the simultaneous eigenstate with eigenvalue $+1$ of all the operators S_i. These operators form a commutative subgroup of the Pauli group named the *stabilizer group* $\mathcal{S}$. Let us now see the formalism in action considering for example the 3-qubit state

$$|\mathrm{GHZ}\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}. \tag{2.3}$$

It is easy to see that the following set of operators

$$\mathcal{S}_{GHZ} = \{I_1I_2I_3, X_1X_2X_3, Z_1Z_2I_3, Z_1I_2Z_3, I_1Z_2Z_3, -X_1Y_2Y_3, -Y_1X_2Y_3, -Y_1Y_2X_3\}, \tag{2.4}$$

stabilize the 3-qubit GHZ state i.e there are 8 operators in the Pauli group satisfying Eq (2.2). Note that if S_i and S_k are two stabilizers then $S_iS_k|\psi\rangle = S_i|\psi\rangle = |\psi\rangle$, thus the product S_iS_k is as well a stabilizer of the state. The complete stabilizer group

of the 3-qubit GHZ state can thus be generated by recursive product of 3 operators:

$$\mathcal{G}_{GHZ} \equiv \{Z_1 Z_2 I_3, I_1 Z_2 Z_3, X_1 X_2 X_3\}. \tag{2.5}$$

The subgroup $\mathcal{G}_{GHZ}$ is called set of generators of the stabiliser group and it is the maximum independent subset of a stabilizer group. In general, given any quantum state the number of stabilizers attached to it may vary, however we define stabilizer states all those n-qubit states whose stabilizer group contains 2^n elements, generated by n generators. Notably, stabilizer states can be defined uniquely from their generator group. This is in essence the power of this simple formalism, and the reason of its applications in most of the research areas of quantum information theory.

2.2 Unitary Operations Within the Stabilizer Formalism

Within the stabilizer formalism unitary operations on stabilizer states correspond to simple transformation rules on the stabilizer operators. However, it should be noted that not all the unitary operations can be described within this formalism but only a restrict class of operations, which map a Pauli operator into another Pauli operator. Such unitary transformations are called *Clifford operations*, and their action on a stabilizer group is described in the following.

Consider a generator group $\mathcal{G} = \{S_i\}$, given the state $|\psi\rangle$ stabilized by the S_i and a Clifford operation U_c, we have:

$$U_c|\psi\rangle = U_c S_i |\psi\rangle = U_c S_i U_c^\dagger U |\psi\rangle = S_i' U_c |\psi\rangle. \tag{2.6}$$

The transformed state $U_c|\psi\rangle$ is then stabilized by the new operator $S_i' = U_c S_i U_c^\dagger$. Hence, to study the evolution of a quantum state $|\psi\rangle$ under a Clifford operation, we can directly map the generators $\langle\{S_i\}\rangle$ to the new generators $\langle\{S_i'\}\rangle$ through the mapping $S_i \rightarrow U_c S_i U_c^\dagger$, and find the unique state stabilized by the new generators which is exactly $U_c|\psi\rangle$. Remarkably, compared with the usual state-vector description where the evolution of a state is encoded in 2^n parameters, the stabilizer-

Operation	Transformations
$U_c = H$	$U_c X U_c^\dagger = Z$ $U_c Z U_c^\dagger = X$
$U_c = R_{\pi/2}$	$U_c X U_c^\dagger = Y$ $U_c Z U_c^\dagger = Z$
U_c =CNOT	$U_c X_c U_c^\dagger = X_c X_t$ $U_c X_t U_c^\dagger = X_t$ $U_c Z_c U_c^\dagger = Z_c$ $U_c Z_t U_c^\dagger = Z_c Z_t$

Table 2.1: Transformation rules for the Hadamard, $\pi/2-$phase and controlled-NOT.

generator description only requires to keep track of the evolution of n operators[1]. Importantly, any Clifford operation can be generated solely by using CNOT, Hadamard, and $R_{\pi/2}$ phase gates whose action on the Pauli operators is shown in table 2.1. Therefore, any circuit where only Clifford gates are allowed, can be decomposed in terms of CNOT, Hadamard, and phase gates and the action of the circuit on any stabilizer state can be efficiently simulated classically within the stabilizer formalism. This is in short the Gottesman-Knill theorem [10], a milestone of quantum computing theory stating that any Clifford operations followed by the Z measurements, can be simulated efficiently with classical computation. The same does not hold for universal quantum computation for which in addition to the Clifford gates a $R_{\pi/4}$ phase-gate is required. In fact, the $R_{\pi/4}$ phase-gate do not map Pauli operators into Pauli operators, therefore cannot be simulated efficiently within the stabilizer formalism.

2.3 Measurements Within the Stabilizer Formalism

We have seen how the stabilizer formalism can easily describe a quantum state and its evolution. We want now to include the effect of measurements to obtain a formally complete description. We assume, without loss of generality, to measure on a n-qubit stabilizer state with generators $\{S_i\}$ some observable $O \in \mathcal{P}_n$ with outcomes ± 1. The easiest scenario occurs when we have $[O, S_i] = 0$ for all the i.

[1]This approach recalls the Heisenberg picture of quantum mechanics, where the states are fixed and the operators evolve in time.

It's straightforward to see that in this case $\pm O$ is itself a stabilizer of the state with outcomes ± 1, which means the state is unchanged after the measurement. However, more in general, O does not commute with one or more of the S_i and the state after the measurement is projected in one of the eigenstates of O. Suppose now, O doesn't commute with both S_1 and S_2 while it commutes with all the other generators. Using the properties of the commutation operation it is easy to verify that $[O, S_1 S_2] = 0$, hence we simply replace the generator S_2 with $S_1 S_2$. What happens to S_1?
First, we can show that the probabilities of the outcomes ± 1 after the measure of O are both equal to $1/2$:

$$p(+1) = \mathrm{Tr}\left[\frac{I+O}{2}|\psi\rangle\langle\psi|\right], \tag{2.7}$$

$$p(-1) = \mathrm{Tr}\left[\frac{I-O}{2}|\psi\rangle\langle\psi|\right]. \tag{2.8}$$

Since $OS_1 = -S_1 O$ and $S_1|\psi\rangle = |\psi\rangle$ we can write:

$$p(+1) = \mathrm{Tr}\left[\frac{I+O}{2}S_1|\psi\rangle\langle\psi|\right] = \mathrm{Tr}\left[S_1\frac{I-O}{2}|\psi\rangle\langle\psi|\right] = p(-1). \tag{2.9}$$

Along with the normalization constraint $p(1)+p(-1) = 1$ the only possible solution is $p(+1) = p(-1) = 1/2$. Given one of the two outcomes, we know that the state after the measurement is projected into $|\psi^*\rangle = \frac{I\pm O}{2}|\psi\rangle$ therefore the new stabilizer generators are given by the list:

$$\{\pm O, S_1 S_2, S_3, ..., S_n\}. \tag{2.10}$$

2.4 Graph States

An important application of the stabilizer formalism deserving a section by itself is to describe the so-called graph states, a sub-group of the stabilizer states. In particular, from an experimental point of view, all the most common states employed in quantum information processing and in this thesis are graph states.

A graph is a collection of vertices and edges connecting them. Exploiting the stabilizer formalism we can uniquely identify some quantum states by means of a

graph according to the following rules:

- Each vertex corresponds to a single-qubit in the state $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$.
- An edge between two vertices corresponds to the 2-qubit gate control-Z (CZ) applied to the two qubits.

Using the rules above, given a graph the corresponding graph state $|G\rangle$ is

$$|G\rangle = \prod_{(l,m)\in E} CZ_{lm}|+\rangle^{\otimes|V|}, \tag{2.11}$$

where the pair of indices (l,m) defines an edge connecting the vertices l and m respectively, E is the set of edges and $|V|$ is the number of vertices. Interestingly, in the stabilizer framework, before applying the CZ operations each vertex is initially in the state $|+\rangle$ stabilized by X and the generator of the state would be simply the list $\langle X_1, X_2, ..., X_n\rangle$. Once we consider the action given by each edge, the generator is transformed by the unitary $U = \prod_{(l,m)\in E} CZ_{lm}$ which means replacing the stabilizer operator X_i with the new operator K_i:

$$K_i = X_i \prod_{j\in V_i} Z_j, \tag{2.12}$$

where V_i is the neighbourhood of vertex i. For instance the graph in Fig. 2.1 with $|V| = 3$ is given by the generators

$$\langle X_1Z_2Z_3, Z_1X_2I_3, Z_1I_2X_3\rangle,$$

which after a Hadamard gate on qubits 2 and 3 becomes

$$\langle X_1X_2X_3, Z_1Z_2I_3, Z_1I_2Z_3\rangle,$$

that is the stabilizer generator of the 3-GHZ state. Therefore we say that the GHZ state is a graph state up to local Clifford (LC) operations (in the example two local Hadamard gates leading to the graph in Fig 2.1). This result turns out to be general and given a n-qubit graph state $|G\rangle$ and a n-qubit stabilizer state $|\psi\rangle$ there exists a

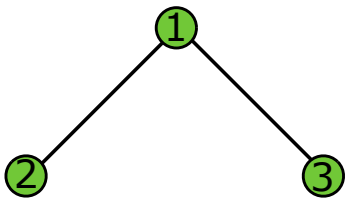


Figure 2.1: **Graph state example.** Shown is a 3-qubit graph state corresponding to the GHZ state up to local Clifford operations.

set of local Clifford operations on the n qubits $\{C_1, C_2, ..., C_n\}$ such that

$$|\psi\rangle = \bigotimes_{j=1}^{n} C_j |G\rangle, \tag{2.13}$$

as it was proven in Ref. [11]. This result was used to show one of the first efficient classical protocols to simulate stabilizer circuits [12] in accordance with the Gottesman-Knill theorem. Note that as in the local Clifford group there are 24 operators (see Ref. [9] for a table of the operators) one of the possible 24^n different n-qubit Clifford unitaries (up to a global phase) must relate a graph state $|G\rangle$ to a given stabilizer state $|\psi\rangle$.

2.5 Graphical Rules for Graph-State Transformations

We have seen in Sec. 2.2 and 2.3 how in the framework of the stabilizer formalism Clifford operations and measurements on stabilizer states follow simple transformation rules. Similarly, some graphical rules exist to account for these operations directly on the graph linked to a graph state.

If an LC operation is applied on qubit α of some graph state $|G\rangle$ the corresponding graph transforms according to the so-called local complementation rule see Fig 2.2. Given some starting graph, the recursive application of the rule will generate the "orbit" of all the graph states equivalent to the initial one under LC. As by definition the amount of entanglement does not increase under local operations and classical communication (LOCC) this graphical formalism is useful to group graph states within the same entanglement class. On the other hand, if two graph states can not be linked by the LC-rule then they are not equivalent under LC, and

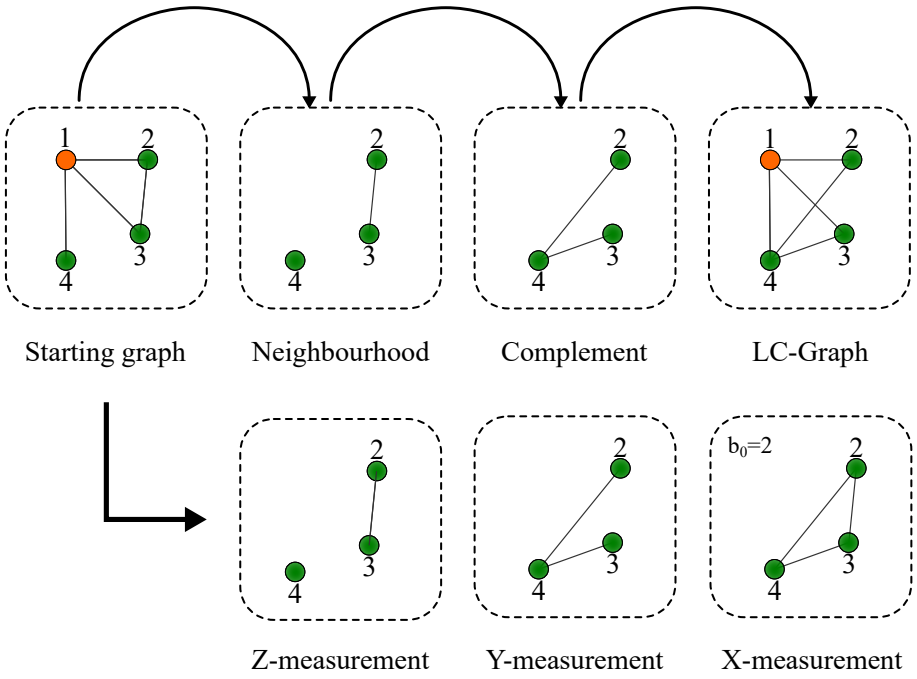


Figure 2.2: **Graphical rules for a LC operation and single measurement on qubit 1.** Starting from the graph shown in the first box from the top-left, the neighbourhood of the vertex 1 is selected (second box), complemented (third box) and finally the LC-graph obtained as shown in the last box. The local unitary on qubit 1 mapping the starting graph to the LC-graph is $U_1 = \sqrt{-iX_1}$ up to a phase given by the local unitary on the neighbourhood qubits $\sqrt{iZ_2}\sqrt{iZ_3}\sqrt{iZ_4}$. One the bottom row the action of local Pauli measurements in shown. The Z measurement simply removes from the graph all the edges connecting vertex 1. The Y measurement consist on a Z measurement on the LC-Graph shown in the top row. The X measurement requires first a random pick of one of the neighbours b_0 of vertex 1, then the LC rule is applied with respect to b_0. The obtained temporary graph is measured in the Y-basis with respect to vertex 1 and finally the LC rule is applied again on vertex 1. The resulting graph is shown in last box of the bottom row.

2-qubit gates are required. For a nice overview of the different orbits and classes of graphs the interested reader is referred to Ref. [13].

The case of a local Pauli projective measurement is show in the bottom row of Fig. 2.2. In general, the graph state obtained after a measurement is the one shown up to a local unitary operation. Moreover, for a sequence of local Pauli measurements, such local unitaries have to be taken into account, when the measured qubit is affected by the unitary. For more details the reader is referred to Ref. [9].

2.6 State Tomography, Fidelity and Entanglement

An essential routine in experimental quantum information is the characterisation of an unknown quantum state by means of quantum measurements on N copies of the state. This is achieved with quantum state tomography algorithms, whose function is to output the density matrix of the unknown state using the obtained data set. Note that, the data set contains enough information to successfully reconstruct the density matrix if the measurements form an informationally-complete set i.e. d^2 measurements for a d-dimensional system. This necessary condition comes from the fact that a d-dimensional system is completely described by a set of $d^2 - 1$ parameters, which can be obtained experimentally from $d^2 - 1$ measurements whose values are then turned into frequencies with one additional measurement. In the following, two different algorithms for state tomography are briefly described.

The simplest algorithm for state tomography is the linear inversion protocol [14, 15]. For a d-dimensional system the idea is to measure on the state describing the system, $n \geq d$ observables $\mathcal{M}_k$ with $k = 1, ..., n$. The observed frequencies f_k, in the case of infinite copies of the state, can be interpreted as the probabilities corresponding to $p_k = \mathrm{Tr}\left[\mathcal{M}_k \rho\right]$ where ρ is the density matrix of the state to reconstruct. In practice of course, with a finite number of samples, the actual probabilities can not be obtained and only an approximation ρ^* of the true density matrix ρ can be computed. The matrix ρ^* is found by solving the equation

$$\rho^* = (S^\dagger S)^{-1} S^\dagger |f\rangle. \tag{2.14}$$

Where the matrix S contains the vectorized measurement operators i.e. a vector containing the columns of the operators $\mathcal{M}_k$ and $|f\rangle$ is the vector of observed frequencies. The matrix $S^\dagger S$ is indeed invertible [15] and the target density matrix ρ^* obtained by simple vectorial operations. This method however suffers the drawback that experimental noise in the data typically leads to unphysical density matrices. We recall that a density matrix has a valid physical meaning if it is semidefinite, Hermitian and with trace one.

This problem can be solved by means of maximum-likelihood estimation algorithms, whose output is the most likely physical density matrix which can reproduce

the observed data [16, 17]. More formally one can consider the function

$$L(\rho) = \prod_{k=1}^{n} P(c_k|\rho), \tag{2.15}$$

where c_k are the recorded raw counts obtained by measuring the observables $\mathcal{M}_k$ and $P(c_k|\rho)$ is the conditional probability of having observed c_k counts given the density matrix ρ. The goal of this method is to search for a matrix ρ^* maximizing Eq. (2.15), and constrained to $\rho^* \geq 0$ and $\mathrm{Tr}\,[\rho^*] = 1$. This problem can be solved numerically as a semidefinite program for example provided by the CVX MATLAB package for specifying and solving convex programs [18].

Once the density matrix is obtained the experimental state can be easily characterised. One important figure of merit is the state fidelity, namely the measure of how close two states are. In particular, if experimentally the setup is prepared to produce the state ρ_{th} and from state tomography on N copies of that state ρ_{exp} is observed, then the quantity

$$F(\rho_{\mathrm{th}}, \rho_{\mathrm{exp}}) = \left(\mathrm{Tr}\left[\sqrt{\sqrt{\rho_{\mathrm{th}}}\rho_{\mathrm{exp}}\sqrt{\rho_{\mathrm{th}}}} \right] \right)^2, \tag{2.16}$$

is a measure of how close the observed and prepared states are [19]. In the expression, $\sqrt{\rho_{\mathrm{th}}}$ is a matrix B satisfying $BB = \rho_{\mathrm{th}}$. In general, some important properties of the function $F(\rho_{\mathrm{th}}, \rho_{\mathrm{exp}})$ are the symmetry $F(\rho_{\mathrm{th}}, \rho_{\mathrm{exp}}) = F(\rho_{\mathrm{exp}}, \rho_{\mathrm{th}})$, its values lie between 0 and 1 where $F(\rho_{\mathrm{th}}, \rho_{\mathrm{exp}}) = 1$ if and only if $\rho_{\mathrm{th}} = \rho_{\mathrm{exp}}$. Another property is the invariance under unitary operations i.e. $F(U\rho_{\mathrm{th}}U^\dagger, U\rho_{\mathrm{exp}}U^\dagger) = F(\rho_{\mathrm{th}}, \rho_{\mathrm{exp}})$, for any unitary operator U. This is sometimes useful in practice, where the state observed might look different from the prepared one but their compatibility — and the accuracy of the experimental setup — can be recovered by simple transformation of ρ_{th} in post-processing. The fidelity in Eq. (2.16) is therefore an important tool in experiments, and is often used as a quick test for characterising experimental setups.

The fidelity however can not measure the amount of entanglement present in a given state. In general, the problem of the entanglement detection for arbitrary states at arbitrary dimension is an hot topic of research by its own and the reader is referred to Refs. [20, 21] for a nice introduction. Here, we discuss some entanglement measures for bipartite 2-dimensional systems. One of the most common is the

concurrence [22, 23] defined as

$$C(\rho) = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}, \tag{2.17}$$

where the λ_i are the decreasingly ordered eigenvalues of the matrix $\sqrt{\sqrt{\rho}\tilde{\rho}\sqrt{\rho}}$, where $\tilde{\rho} = (\sigma_y \otimes \sigma_y)\rho(\sigma_y \otimes \sigma_y)$. Experimentally, this quantity can be easily computed using the density matrix of the system obtained from state tomography. Another measure easy to compute is the negativity, whose definition is directly derived from the Peres–Horodecki criterion [24]: a necessary condition (and sufficient in the 2x2 and 2x3 dimensional cases), for the joint density matrix ρ to be separable. The negativity is defined as

$$N(\rho) = \frac{||\rho^{T_A}||_1 - 1}{2}, \tag{2.18}$$

where $||...||$ is the trace norm of the partially transposed state. In the following, and in particular in Chapter 6, this quantity will be extensively used as an entanglement quantifier.

Finally, entanglement can also be established between the principal system and its environment, although from the system's point of view this is often accounted as quantum noise (an overview on this subject will be given in Chapter 6). If this happens, the performance of the states in most of the typical quantum information tasks is degraded. The quantity accounting for this phenomenon is the state purity, simply defined as

$$\mathcal{P}(\rho) = \mathrm{Tr}\left[\rho^2\right]. \tag{2.19}$$

This quantity measures the purity of the system whose density matrix ρ satisfies $\mathcal{P}(\rho) = 1$ if $\rho = |\psi\rangle\langle\psi|$ whereas $\mathcal{P}(\rho) < 1$ if the density matrix is a mixture of pure states. Physically, the purity of a state is degraded by the erasure of information required to characterise the state itself. An instructive example is a general quantum measurement M_m whose outcome m is lost. According to quantum mechanics the state of the system after the measurement is $\rho'_m = M_m \rho M_m^\dagger / p(m)$ where $p(m) = \mathrm{Tr}\left[\rho M_m^\dagger M_m\right]$ is the relative probability. If the value of the outcome m is unknown,

the system can be described by the mixture

$$\sum_m p(m)\rho'_m = \sum_m M_m \rho M_m^\dagger. \tag{2.20}$$

This last expression will be recurrent in Chapter 6 to describe the action of a noisy channel on a quantum state.

Chapter 3

Building Blocks for Multi-qubit Graph States

In the previous Chapter we have seen from a theoretical point of view what is a graph state and why it is useful in quantum information. In this Chapter, I present a manual for building non-trivial multi-qubit graph states out of an experimentalist's photonic toolkit. This contains standard optical elements such as a laser, a number of mirrors, beam splitters, polarisers, lenses and wave-plates, as well as more expensive equipment such as non-linear crystals and single-photon detectors. Resembling a kid playing with Lego, the experimentalist's job is to assemble those components into more complex photonic setups, whose working principle will be the subject of this chapter.

I will describe in Sec. 3.1, the probabilistic single-photon sources employed for all the results shown in this thesis. The main quality factors to look for in single-photon sources are the so-called: photons' spectral purity, multi-mode generation, and multi-pair creations which I present in Sec 3.2, Sec 3.3, and Sec 3.4, respectively. In Sec 3.5, an instance of a 2-qubit entangled state in polarisation is presented. Starting from that, I describe in Sec 3.6 the so-called fusion gate, that is the main ingredient for scaling to multi-qubit graph states. Finally, in Sec. 3.7 I describe the general scheme to prepare with a photonic platform the graph states employed throughout this thesis.

3.1 Single-Photon Sources

Single-photon sources assume a key role in modern quantum technologies. The ideal single-photon source is an on-demand, deterministic, source delivering light pulses in a well-defined polarization and spatio-temporal mode, and containing exactly one photon [6, 25]. Many physical realisations have been proposed so far, but a truly single-photon source has not been realised yet. However, even without a truly single-photon source many applications can be realised within the limits imposed by realistic sources e.g. limited time to complete a quantum protocol, before the quality of the photons degrades irrecoverably.

One popular approach is based on materials behaving as two-level systems. The earliest implementations were obtained with atoms [26], ions [27] or molecules [28], lately replaced by artificial atoms in a solid-state environment as for example quantum dots using III-V semiconductors [25]. Albeit these platforms are expected to eventually fulfil the definition above of a single photon source, they still face important challenges. The two main road-blocks are the limited extraction efficiency i.e. the probability that a photon emitted from the dot is extracted and coupled into fibre, and the limited indistinguishability i.e. the photons emitted from different trials are not identical in all degrees of freedom. Nevertheless, state-of-the-art quantum dots [29, 30] can achieve up to 60% extraction efficiency, single-photon purity of 97.5% and indistinguishability between two consecutive emissions of 97.5%. Yet, the scalability of these sources for multi-photon experiments is still an open question due to intrinsic coupling with the solid-state environment.

Other very popular single-photon sources exploit instead non-linear effects to probabilistically produce single photons. These probabilistic single-photon sources are based on either *spontaneous parametric down-conversion* (SPDC), a second-order non-linear process, or on four-wave mixing a third-order non-linear process [31, 32]. In the following and throughout this thesis we will only consider SPDC sources. This type of sources have the advantage of being realised by a fairly simple setup, only consisting of a laser beam and a non-linear crystal working at room temperature. The main disadvantage is instead that they can not deliver on-demand, deterministic single photons. Yet, they have been historically the most used sources for milestones experiments in quantum information, and they remain the first candidate

to implement multi-photon photonic platforms as those presented in this thesis.

Because of non-linearities in the atoms' response, formally described by the susceptibility $\chi^{(2)}$, a pump photon of frequency ω_p is destroyed while two photons of frequencies ω_s, ω_i are simultaneously created from the vacuum state. As the energy and the momentum of the entire process must be conserved it follows:

$$\omega_p = \omega_i + \omega_s \tag{3.1}$$

$$\vec{k_p} = \vec{k_i} + \vec{k_s}, \tag{3.2}$$

also known as phasematching equations. The two down-converted photons ω_s, ω_i generated by spontaneous emission are by convention called *signal* and *idler*, respectively. We note that in spontaneous PDC idler and signal are seeded by the vacuum component of the electromagnetic field, and therefore have a low probability to be generated. This is opposed to the *stimulated* PDC, where the idler and signal once generated become in turn the seeds for more pairs, leading to high-probability of photon generation [7]. However, as the key point is to have a single-photon source the low-gain spontaneous PDC has been preferred to stimulated PDC.

The $\chi^{(2)}$ non-linearity arises from the lack of a centre of inversion symmetry in the crystal, leading to a dependence of the crystal's refractive index on the polarisation of the light propagating within it, an effect also known as optical birefringence. As a result of this, different types of PDC are categorized by the polarizations of the input photon and the two output photons. If the idler and signal share the same polarisation of the pump, the process is named type-0 PDC. When instead the polarisation of idler and signal is the same, but perpendicular to the pump's polarisation we have type-I PDC and finally, when idler and signal have perpendicular polarisation is a type-II PDC. Moreover, we say the process is *degenerate* or *non-degenerate*, whether the emitted photons have the same energy $\omega_s = \omega_i$ or not.

In the following, we will consider only *degenerate collinear type-II parametric down-conversion* obtained using a potassium titanyl phosphate (KTP) non-linear material.

We consider the scenario whereby the presence of one photon e.g the signal is heralded by the detection of the second e.g. the idler. Therefore, the quality of

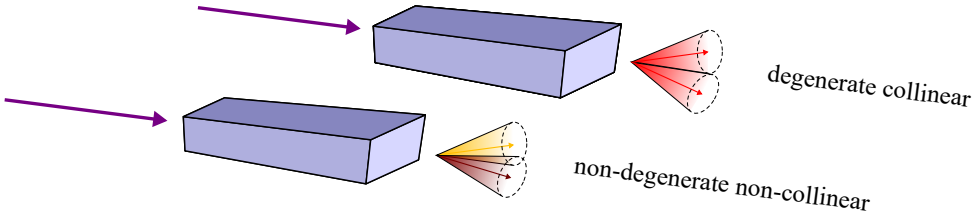


Figure 3.1: **Parametric down-conversion nomenclature.** Idler and signal directions and wavelength must satisfy the conservation rules of energy and momentum. If the momentum of the photons has a different direction from the pump, the process is called non-collinear, whereas if the direction is conserved is named collinear. When the idler and signal have different wavelengths is a non-degenerate down-conversion, it is degenerate otherwise.

the source is directly linked to the reliability of this process defining two important figures of merit: heralding efficiency and brightness. Moreover, note that when we trigger a detector by detecting the heralded photon, we are formally tracing out the information contained in its quantum state. In the ideal case where the two-photon state is separable, the trace operation does not effect the target single photon state which will be preserved pure. However, if (spectral)correlations between the idler and signal were contained in the two-photon state, the herald detection will lead to mixture in the remaining single photon, corrupting its purity.

In the following sections, we review the standard quality factors of PDC sources and how to improve them experimentally.

3.2 Spectral Purity

One of the main roadblocks to scalability of SPDC sources is the presence of intrinsic spectral correlations between the idler and signal photons. As we will see such correlations can severely limit the quality of multi-photon entangled states and therefore their usefulness.

The SPDC state in terms of the photons' spectrum is obtained from the first-order term in the Dyson series expansion of the evolution operator [33], the 1-pair quantum state in the Fock space can be then written as:

$$|\Psi\rangle_{s,i} = A \iint d\omega_i d\omega_s \, f(\omega_i, \omega_s) a^\dagger b^\dagger |0\rangle_i |0\rangle_s. \tag{3.3}$$

In the equation A is some normalisation constant, $f(\omega_i, \omega_s)$ is the so called joint spectral amplitude (JSA) and a, b are the idler and signal modes respectively. The JSA plays a fundamental role as it contains all the spectral correlations between the idler and signal. It can be expressed as:

$$f(\omega_s, \omega_i) = \alpha(\omega_i, \omega_s)\phi(\omega_i, \omega_s), \tag{3.4}$$

where $\alpha(\omega_i, \omega_s) = \alpha(\omega_{p_0} - \omega_i - \omega_s)$ is the pump envelope centred on ω_{p_0} given by

$$\alpha(\omega_i, \omega_s) = \int_{-\infty}^{+\infty} dt \ \mathrm{sech}[\frac{t}{\tau}]e^{i\Delta\omega t} = \sqrt{\frac{\pi}{2}}\tau \ \mathrm{sech}[(\omega_{p_0} - \omega_i - \omega_s) * \frac{\pi\tau}{2}], \tag{3.5}$$

where τ depends on the pulse's full-width half-maximum (FWHM). The function $\phi(\omega_i, \omega_s)$ is called phase matching function (PMF) and it depends on the non-linearity of the medium and the phase mismatch. The PMF is what effectively determines the spectral purity of the single photons produced, and it can be expressed as:

$$\phi(\omega_i, \omega_s) = \int_{-\infty}^{+\infty} dz \, g(z)e^{i\Delta k(\omega_i, \omega_s)z}, \tag{3.6}$$

where $\Delta k(\omega_i, \omega_s) = k_p(\omega_i + \omega_s) - k_i(\omega_i) - k_s(\omega_s)$ is given by the material dispersion, $g(z) = \chi^2(z)/\chi_0^2$ is given by the normalized susceptibility. In a bulk non-linear crystal, the $g(z)$ is simply a step function non-zero only from $-L/2$ and $L/2$, where L is the crystal's length. In this case Eq. (3.6) reduces to

$$\phi(\omega_i, \omega_s) = \mathrm{sinc}\left(\frac{\Delta k(\omega_i, \omega_s L)}{2}\right). \tag{3.7}$$

The PMF is therefore maximum when the condition $\Delta k(\omega_i, \omega_s) = 0$ is satisfied. As the $\Delta k(\omega_i, \omega_s)$ intrinsically depends from the atomic structure of the crystal itself [34], the phase matching condition might not be always satisfied. One solution is to periodically alternate the pooling of the crystal between $+1$ and -1 every coherence length with a period Λ, keeping the domain width constant. This approach can be applied to a KTP crystal leading to periodically-poled KTP (PPKTP) crystals, as those employed for the experiments shown in this thesis. In this case, the PMF

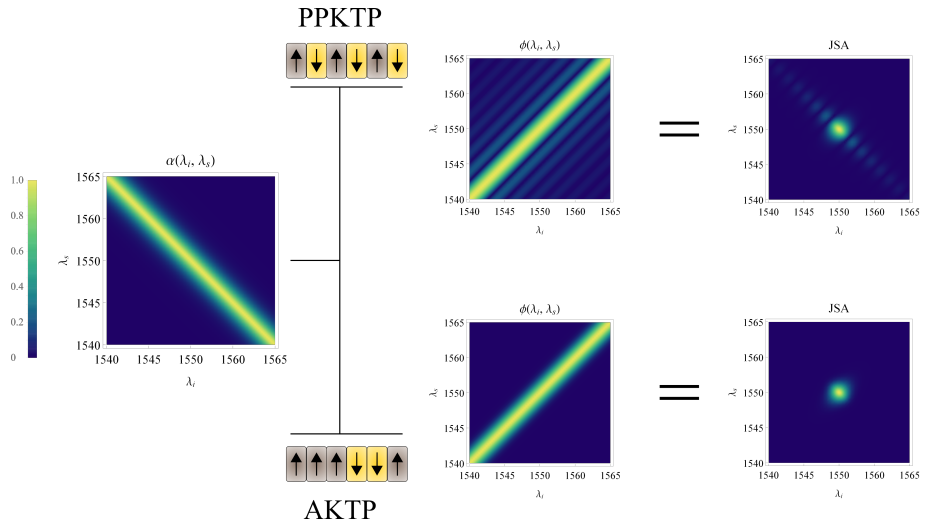


Figure 3.2: **Comparison between a standard PPKTP and an apodized crystal.** The former alternates consecutively a domain with upward orientation and one with downward orientation, keeping the domains' width constant. This leads to a sinc-type PMF, which when multiplied with the pump envelope produces correlations in the JSA. The latter, instead, employs a custom orientation of the domains together with a variation of their width. The resulting PMF is Gaussian and the JSA cleaned from side lobes and unwanted spectral correlations.

is

$$\phi(\omega_i, \omega_s) = \text{sinc}\left[(\Delta k(\omega_i, \omega_s) - \frac{2\pi}{\Lambda})\frac{L}{2}\right] e^{i(\Delta k(\omega_i,\omega_s) - \frac{2\pi}{\Lambda})\frac{L}{2}}, \tag{3.8}$$

therefore the value of Λ adds a degree of freedom to fulfil the phase matching condition $\Delta k(\omega_i, \omega_s) - \frac{2\pi}{\Lambda} = 0$. However, we note that the optimal value for Λ depends on the wavelength and not all the values of Λ can be achieved in practice.

Sadly, the JSA as in Eq. (3.4) is not separable with this choice of PMF i.e. $f(\omega_i, \omega_s) \neq f_i(\omega_i) f_s(\omega_s)$. Hence whenever either the idler or signal are traced out (following a detection) the remaining photon is in a mixed state in the spectrum.

The simplest and most common approach to mitigate this effect, is by filtering the two photons with a narrow-band filter. The filters effectively cut off the side lobes of the PMF — and therefore of the JSA — increasing the spectral purity at the cost of reducing the state's photon number purity [35] as well as the heralding efficiency [36].

An alternative method recently refined by our group [37] following previous works [38–40], addresses the non-linearity profile $g(z)$ of the crystal which is suitably shaped through domain-engineering techniques. In particular, if the non-linear profile is carefully engineered, a Gaussian-like PMF perpendicular to the pump en-

velope is obtained, leading to a separable JSA function, see Fig. 3.2. This is achieved by varying the width and the orientation of the crystal's domains, an optimization problem solved by adapting an annealing-based algorithm introduced by Reid *et al.*[41]. The advantage of this method is the possibility of employing these sources without any spectral filtering and its drawbacks. A comparison between a PPKTP and an apodized crystal is shown in Fig. 3.2.

The method was experimentally demonstrated in our group and the reader is referred to Appendix A for further details.

3.3 Multi-mode PDC

The single-photon source based on PDC is realised upon detection of one photon to herald the presence of the other. In practice however, before the detection, photons are typically coupled into single-mode fibre whose action is comparable to a filter for the photons' spatial modes. This leads to limited coupling efficiency, thus degrading the quality of the single-photon source to be used. In the following, we review the problem of the multi-mode generation in PDC and how to prevent it by accurate engineering of the experimental setup.

We consider a multi-mode two-photon quantum state

$$|\psi\rangle = \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} \psi(m,n)\, a_m^+ b_n^+ |00\rangle, \tag{3.9}$$

where m and n are indices corresponding to the available modes according to the distribution $\psi(m,n)$ for particle a and b respectively. In general a mode can be spatial, temporal, spectral, polarisation or any other mode corresponding to a degree of freedom of the particles. For the purposes of this section we consider the available spatial modes of the single photons described by the Hermite-Gauss modes TEM_{pl} and for compactness we identify the indices m and n in Eq (3.9) as the pairs $m \equiv (p_a, l_a)$ and $n \equiv (p_b, l_b)$ for photons a and b respectively. With this notation, the spatial Gaussian mode TEM_{00} corresponds to $m = n = 0$. In the following, we assume ideal detectors and focus our study on the effects of single-mode coupling to the quality of single-photon PDC sources.

Before diving into the main claim, we recall that in general the modes available

for propagation in a fibre are given by solving the Helmholtz equation for waves, derived from the Maxwell equations when some boundary conditions are set

$$\nabla^2 f = -k^2 f, \tag{3.10}$$

where k is the wave-number. The eigenfunctions f are characterized by a specific set of parameters to describe the propagation characteristics as a unique entity such as spatial distribution for each field component, an effective refractive index, and the optical power distribution for each of the propagating modes. In step-index optical fibres the eigenfunctions can be found analytically and are the so called linearly polarized (LP) modes shown in Fig 3.3. Single-mode fibres are fabricated such that only the mode LP_{01} can propagate throughout the fibre. As the LP_{01} mode presents an intensity profile with a good overlap to the Hermite-Gaussian TEM_{00}, this is the only transmitted in a SMF.

Hence, in our two-photon state in Eq (3.9), only the component given by $\psi(0,0)$ will generate a coincidence event i.e. both photons are coupled and transmitted into fibre leading to the click of both detectors within some time window δt. Assuming no losses in fibres and ideal detectors, the coincidence event happens with probability

$$P_{ab} = |\langle 00|a_0 b_0|\psi\rangle|^2 = |\psi(0,0)|^2. \tag{3.11}$$

The total probability of particle a alone to be in the mode $m = 0$ is therefore

$$P_a = P_{ab} + \left|\langle 00|a_0 \sum_{n=1}^{\infty} b_n|\psi\rangle\right|^2 = P_{ab} + \left|\sum_{n=1}^{\infty} \psi(0,n)\right|^2, \tag{3.12}$$

similarly the probability for particle b to be in the mode $n = 0$ is

$$P_b = P_{ab} + \left|\langle 00|b_0 \sum_{m=1}^{\infty} a_m|\psi\rangle\right|^2 = P_{ab} + \left|\sum_{m=1}^{\infty} \psi(m,0)\right|^2. \tag{3.13}$$

From these expressions we can define the probability that particle a(b) is in mode

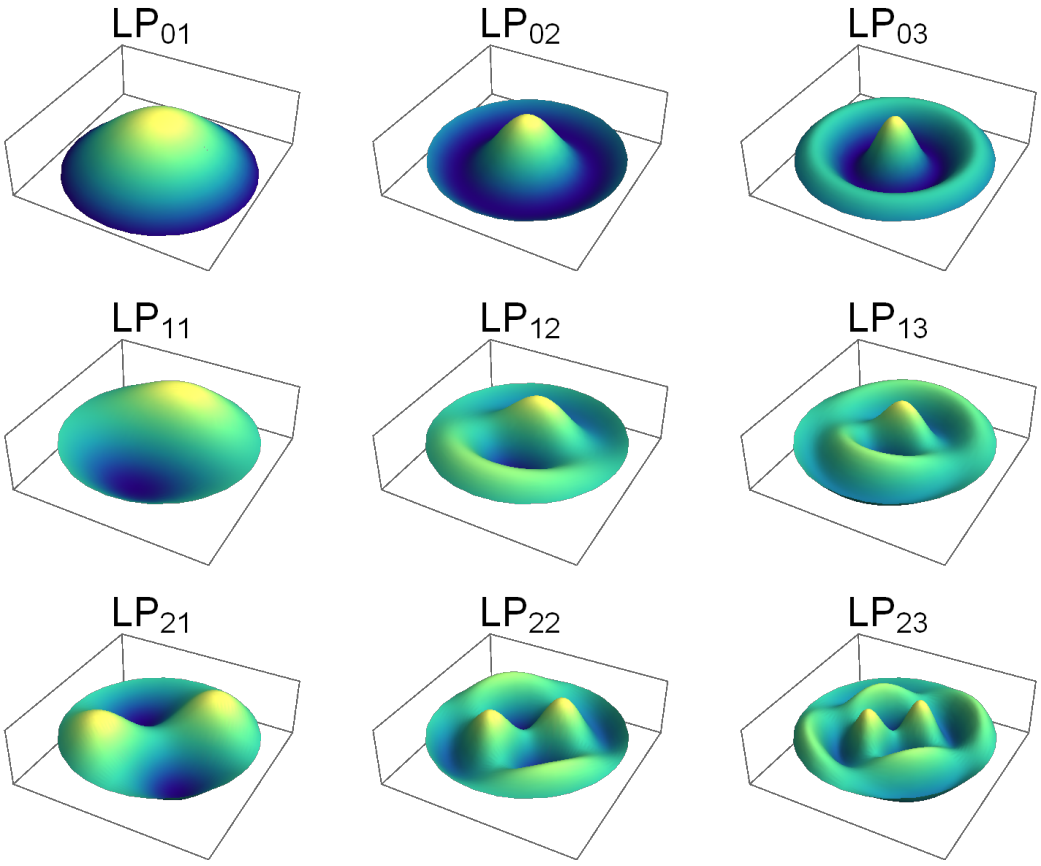


Figure 3.3: **LP modes of a single mode fibre** Shown are representations of the LP spatial modes. They are derived from Bessel functions at different orders. The axis are not shown as irrelevant for the purpose of this representation, but they can be seen as parametric functions revolved around the Z-axis.

$m = 0 (n = 0)$ conditioned on particle b(a) being in mode $n = 0 (m = 0)$

$$P_{a|b} = \frac{P_{b|a} P_a}{P_b} = \frac{P_{ab}}{P_b}, \tag{3.14}$$

$$P_{b|a} = \frac{P_{a|b} P_b}{P_a} = \frac{P_{ab}}{P_a}. \tag{3.15}$$

The coupling efficiency can thus be defined as

$$\eta_c = \sqrt{P_{a|b} P_{b|a}} = \frac{P_{ab}}{\sqrt{P_a P_b}}, \tag{3.16}$$

which in the ideal case is equal to 1. However, in practice a value lower than 1 will be observed due to two main factors: photons loss from their generation to detection and non-zero probability of generating photons in a mode mismatched with the target LP_{01}. Whereas the losses in fibre can not be controlled, the coupling

efficiency η_c can be increased by the experimental control of the pump's beam size when focussed into the crystal, as will be explained in the following.

3.3.1 Experimental Control of Brightness and Heralding

Heralding efficiency and brightness are the two most frequently cited factors to benchmark the quality of a probabilistic single photon-source. In essence, the former quantifies the probability that after the detection in one mode of one photon from the non-linear process, another photon is present in the other mode. The latter instead quantifies how many pair of photons are generated by the source. In particular, this is expressed as the number of detected pairs per mW of pump power and per second.

Experimentally, the heralding efficiency is directly linked to the coupling efficiency in Eq. (3.16) and it can be obtained from the raw counts as

$$\eta_c = \frac{cc}{\sqrt{s_a s_b}}, \tag{3.17}$$

where cc are the coincidence counts, s_a and s_b single counts for photons a and b respectively. This is often called the *heralding efficiency*, whereas the quantity given by the number of cc per mW of pump power and per second is named *brightness*.

The problem of the heralding and brightness dependence on the experimental parameters typically involved in SPDC sources, was formally tackled by Bennink [42]. For a related experimental study see Ref. [43]. The model presents a study of SPDC for the case in which the pump and collecting optics define collinear Gaussian spatial modes. The heralding and brightness are studied in terms of the dimensionless focusing parameter ξ defined as

$$\xi = \frac{L}{kw^2}, \tag{3.18}$$

where L is the crystal's length, k and w the beam wave number and waist respectively. In the SPDC three beams are involved: the pump beam with focusing parameter ξ_p, and idler and signal with parameters ξ_i and ξ_s respectively. According to the model proposed by Bennink and under the assumptions therein, heralding and brightness are maximized when $\xi_p \approx \xi_i \approx \xi_s$, imposing restrictions on the collection waists respect to the pump focusing waist i.e. the idler and signal waist should

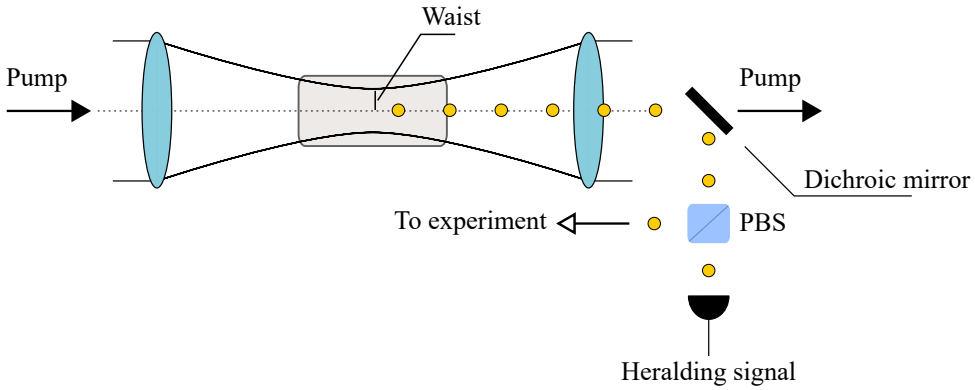


Figure 3.4: **Experimental scheme.** The pump beam is focussed into the non-linear crystal to generate single photons. A dichroic mirror only reflects single photons subsequently split into two spatial modes by a PBS. One photon is employed as herald, the other as the heralded single-photon to be used as a resource.

be half the size of the pump. In particular, it is interesting to reformulate Eq. 3.18 in terms of the Rayleigh length z_R which essentially, determines the depth of focus. Given that $z_R = \pi w^2/\lambda$ we obtain

$$\xi = \frac{L}{2z_R}, \tag{3.19}$$

therefore from a physical point of view the ξ parameter accounts for the fraction of the crystal effectively interacting with the focussed beam. The condition $\xi_p \approx \xi_i \approx \xi_s$ therefore suggests that the Rayleigh length for the pump, idler and signal should be equivalent. From a physical point of view, if this condition is not met, it means that the idler/signal and pump beams effectively interact with different portions of the crystal, degrading the phase matching.

Notably, it was shown that in the loosely focused pump regime ($\xi_p << 1$) values of heralding efficiencies close to 1 can be achieved although trading-off the brightness of the source. On the other hand, in the regime where $\xi_p >> 1$ very high brightness can be obtained at the cost of low heralding. Using the expression of ξ in terms of the z_R the former condition means that the beam is not diverging within the crystal therefore the wave vector of the beam is parallel to the crystal leading to a single mode. The latter condition instead suggests that when the beam starts diverging within the crystal, the consequent spreading of the wave vector in different directions give rise to multimodes playing against the heralding efficiency. This result was experimentally verified with our sources in a simple setup as sketched in Fig 3.4. The

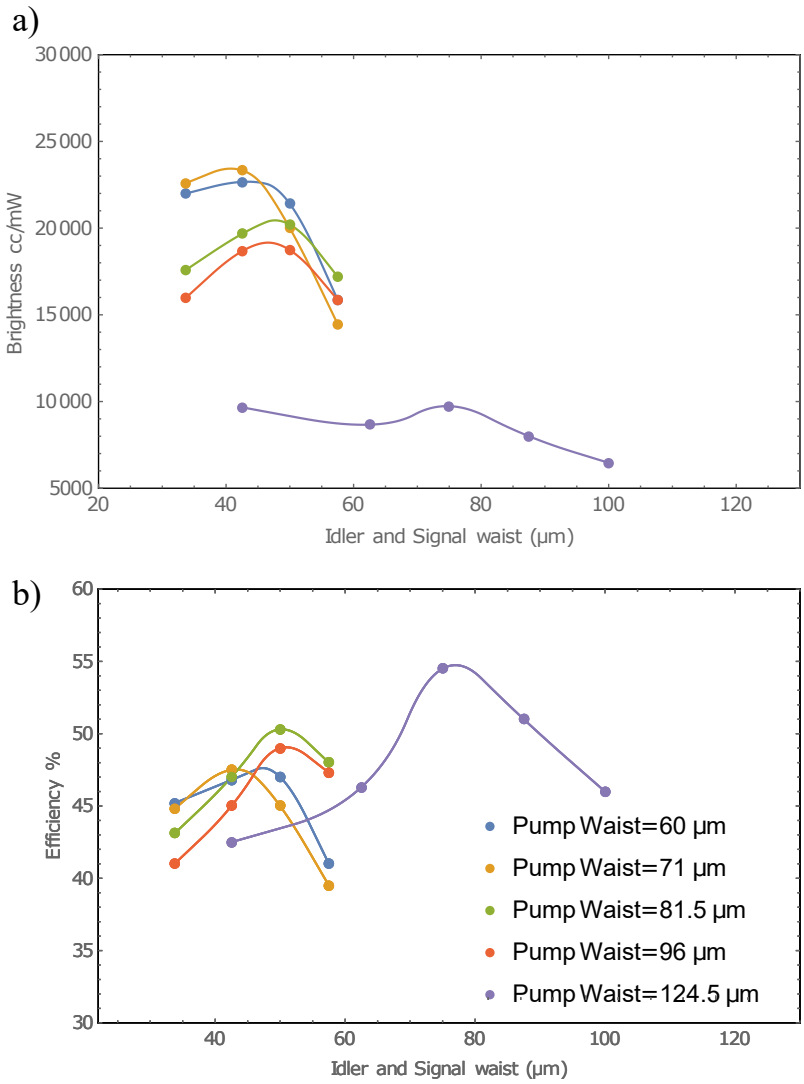


Figure 3.5: **Brightness and heralding optimisation for PDC sources.** The experimentally observed values of brightness (a) and heralding efficiency (b) are shown for different values of the pump waist, spanning from tight-focus to loose-focus. Increasing the pump waist increases the heralding efficiency decreasing the source brightness and vice versa. For each curve the maximum is obtained when the idler and signal waists are $\approx 65\%$ of the pump waist.

pump beam is focussed into the crystal with a lens whose focal length sets the waist of the beam into the crystal and thus the value of ξ. The pump is therefore filtered out with a dichroic mirror and the idler and signal photons split by a polarisation beam splitter (PBS). The transmitted photon is detected and plays the role of the herald, whereas the other single-photon can in general be used for any task. Only the events where eventually both photons are detected count as a coincidence event however, due to either mode-mismatch (as explained in the previous section) or photon loss, one of the photons is not detected leading to a single event and playing

against the heralding efficiency as clear from Eq. (3.17). We experimentally vary the beam size of both the pump and the idler and signal and obtain the results in Fig 3.5. Heralding efficiencies up to 55% can be reached for larger beam size in the crystal, albeit decreasing the brightness as shown in the left-hand side panel of the figure. The observed trade-off is in accordance with the predictions of the Bennink model. For all the experiments reported in this thesis, sources were prepared with settings leading to heralding efficiencies in a range of 50% to 60% and photon pairs per mW per second, spanning from 8000 to 4000. Note, that the reported values for the heralding efficiency are upper bounded by the limited detector efficiency. In fact, in our case, the detectors employed have an estimated 80% detection efficiency leading to a an upper bound on the heralding of 80%. Therefore, in our case, an observed heralding efficiency of 60% is equivalent to an heralding efficiency of 75% in the ideal case.

3.4 Multi-pair Generations in SPDC Sources

In this section we focus our attention on the SPDC state representation in the Fock space. This is particularly useful for understanding one of the main limitations of PDC sources, namely the non-zero probability of generating more than one pair, which is a typical source of noise in many quantum information processing tasks. We denote as $a^\dagger$ and $b^\dagger$ the creation operators for the idler and signal modes respectively. In general an n-photon state for idler and signal can be written as

$$|n\rangle_i = \frac{(a^\dagger)^n}{\sqrt{n!}}|0\rangle_i, \tag{3.20}$$

$$|n\rangle_s = \frac{(b^\dagger)^n}{\sqrt{n!}}|0\rangle_s, \tag{3.21}$$

where $|0\rangle_i$ and $|0\rangle_s$ are the vacuum state for the idler and signal respectively. With this notation, the SPDC state can be expressed as [44, 45]:

$$|\Psi_{\text{SPDC}}\rangle = \sqrt{1-\gamma^2}\sum_{n=0}^{\infty}\gamma^n|n\rangle_i|n\rangle_s. \tag{3.22}$$

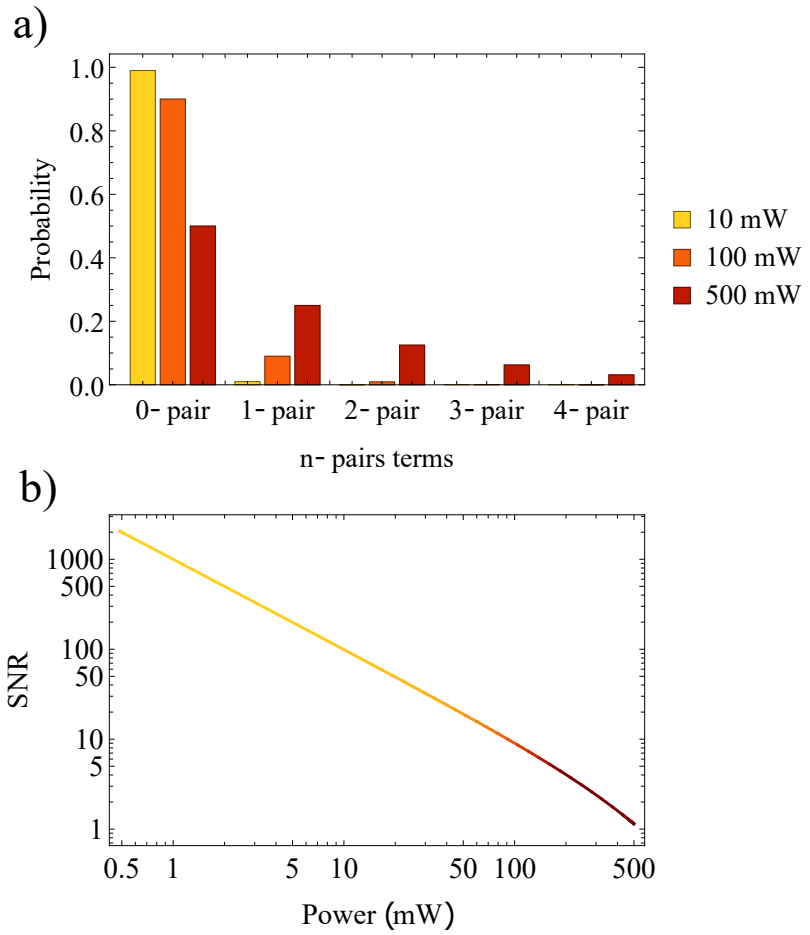


Figure 3.6: **a)Probability for n-pair components.** The probability $P_{\text{pair}}(n)$ is shown for the cases $n = 0, 1, 2, 3, 4$ at increasing power. **b) SNR as a function of pump power.** The value of SNR is shown for increasing pump power. For both figures, a value of $\tau = 10^{-3}$ was set.

The parameter $\gamma = \sqrt{p\tau}$ depends on the pump power p and the constant τ is determined by the light-matter interaction. The probability $P_{\text{pair}}(n)$ of generating an n photon pair per pulse is therefore

$$P_{\text{pair}}(n) = (1 - p\tau)(p\tau)^n. \tag{3.23}$$

The top panel in Fig 3.6 shows the values of Eq (3.23) for $n \in [0, 1, 2, 3, 4]$ and fixed $\tau = 10^{-3}$. For each value of n three different powers are compared: 10 mW, 100 mW and 500 mW shown in yellow, orange and red respectively, only for the vacuum component the probability decreases as the power increases due to the normalisation constraint $\sum_{n=0}^{\infty} P_{\text{pair}}(n) = 1$.

An important figure of merit often considered, is the signal-to-noise ratio (SNR)

defined as

$$\mathrm{SNR} = \frac{P_{\mathrm{pair}}(1)}{\sum_{n=2}^{\infty} P_{\mathrm{pair}}(n)} = \frac{P_{\mathrm{pair}}(1)}{1 - P_{\mathrm{pair}}(1) - P_{\mathrm{pair}}(0)} = \frac{1}{p\tau} - 1, \tag{3.24}$$

that is, the ratio of the n=1 component over the sum of all the other non-zero components. This definition is useful for those applications of SPDC sources, where only the n=1 component leads to the expected results whereas all the $n > 1$ terms are assumed as noise[1]. As shown in the bottom panel of Fig 3.6 the SNR can be increased by decreasing the pump power. Note that, in this limit, the raw generation rate given by $R \times P_{\mathrm{pair}}(1)$ (where R is the repetition rate of the laser) tends to 0 as $P_{\mathrm{pair}}(1) \to 0$. In practice, this is not sustainable as would require infinite amount of time for data acquisition. Therefore, from an experimental point of view, although a high SNR value is recommended this should be traded off with a sensible value of $P_{\mathrm{pair}}(1)$.

Another experimental technique employed to increase the SNR is to temporal multiplex the pump beam, increasing its repetition rate of a factor 2^l for some integer l. The working principle of the temporal multiplexing is sketched in left-hand side of Fig 3.7. Formally this corresponds to the mapping $p \to \frac{p}{2^l}$ and $R \to 2^l R$ obtaining

$$SNR = \frac{2^l}{p\tau} - 1. \tag{3.25}$$

Therefore the SNR increases with the number of multiplexed steps l. Moreover, the ratio β_n of the multiplexed raw generation rate $2^l R P_{\mathrm{pair}}(1)$ with respect to the case without multiplexing, given a n-pair component is

$$\beta_n = \frac{2^l R(1 - \frac{p}{2^l}\tau)(\frac{p}{2^l}\tau)^n}{R(1 - p\tau)(p\tau)^n} = \frac{\left(\gamma^2 - 2^l\right)\left(\gamma^2\right)^{-n}\left(\gamma^2 2^{-l}\right)^n}{\gamma^2 - 1}. \tag{3.26}$$

For $\tau = 10^{-3}$ and different values of l, the above function is shown in the right-hand side of Fig. 3.7 for $n = 1$ and $n = 2$ respectively. Increasing the repetition rate of the pump laser therefore enhances the quality of the single-photon source, suppressing the high order terms and increasing the generation rate of the n=1 component. However, it should be noted that the simple model here presented is incomplete:

[1]Note that this is the worst case scenario. In some applications multi-pair components might lead to expected results too.

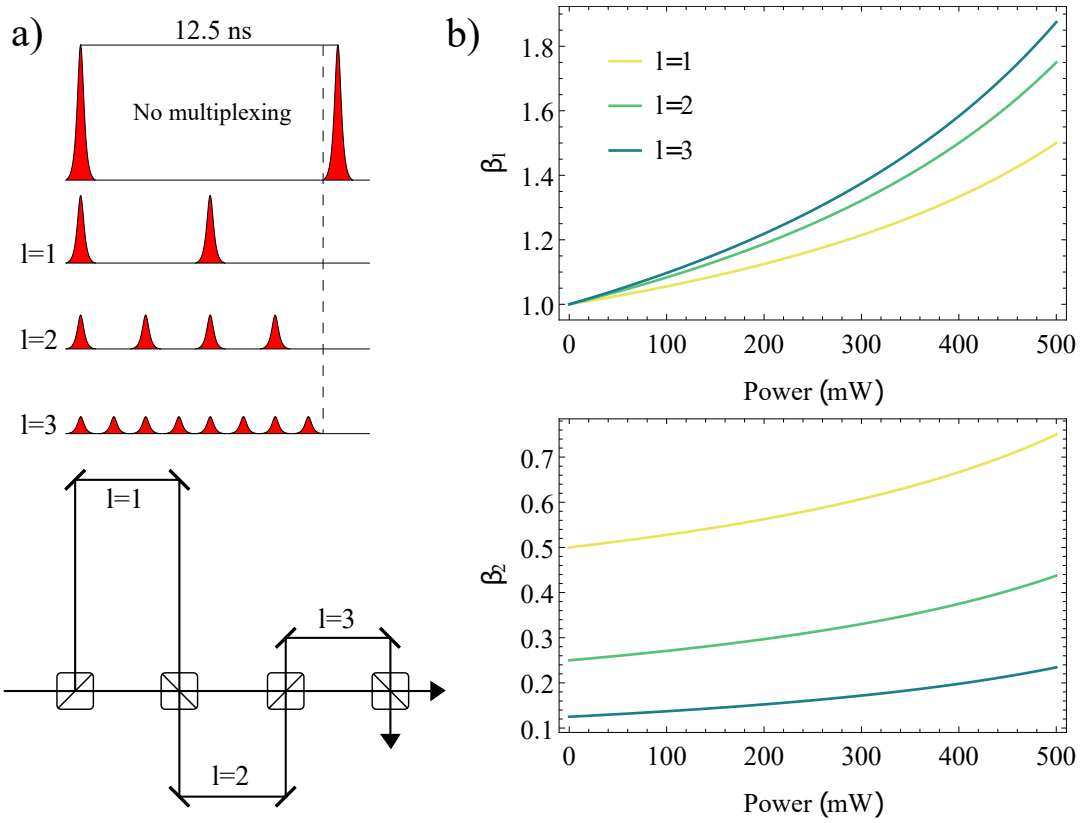


Figure 3.7: **a) Multiplexing scheme** A series of beam splitters split the input beam and recombine it to double the repetition rate every multiplexing step. After three steps at the output the repetition rate is x8 of the initial one, but also the power per pulse is 8 times smaller. **b) Relative generation rate.** The functions β_1 (top) and β_2 (bottom) are shown in a typical range of pump powers for $l = 1$ (yellow), $l = 2$ (green) and $l = 3$ (blue). Notably, for the 1-pair case β_1 is greater than one and increasing with n.

losses and more importantly inefficient detectors should be included.

In the experimental results presented in this thesis, a temporal multiplexing technique with $l = 2$ was employed. Moreover, observations suggest that an ideal condition of SNR and $P_{\text{pair}}(1)$ is achieved with a pump power $p \approx 100mW$, which will be the typical value employed for the experiments reported in this thesis.

3.5 Polarisation-entanglement Sources

In order to employ a collinear type-II crystal as a source of entangled photons, we follow the well established scheme introduced by *Fedrizzi et al.* [46]. The non-linear crystal is embedded within a Sagnac interferometer, whose output — when a 1-pair

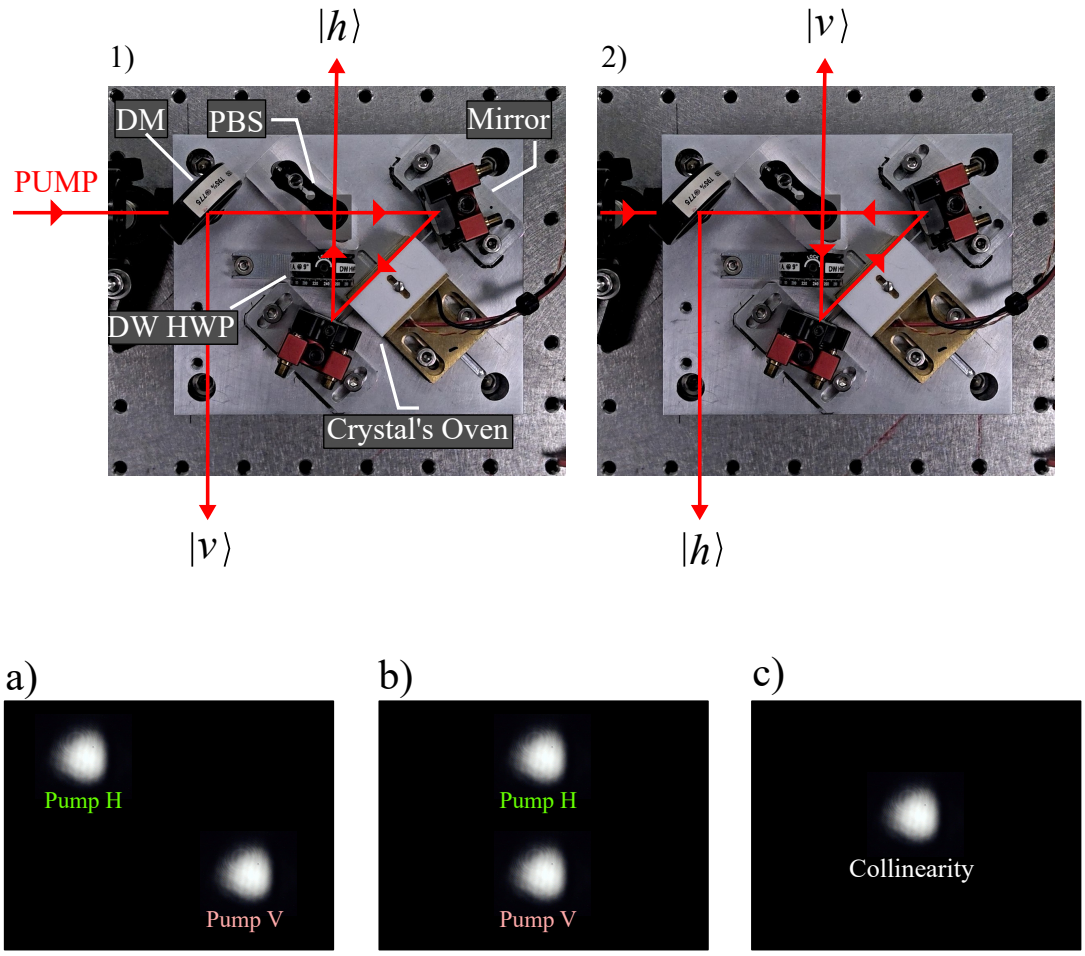


Figure 3.8: **Polarisation-entanglement sources.** The top row in the figure shows a picture from the top of an entanglement source with its components. The pump is transmitted by a dichroic mirror (DM), then depending on the pump's polarisation it travels clockwise or anticlockwise in the sagnac interferometer. If the pump is horizontally polarised as in 1), it is transmitted by a PBS, directed by a mirror into the crystal (inside the oven), then a second mirror it is used to close the loop at the PBS. The dual-wavelength HWP (DW HWP) rotates the pump from horizontal to vertical so that at the PBS is reflected back to the pump laser. At the point where the pump interacts with the crystal a pair of orthogonally polarised single photons is created, the $|h\rangle$ photon is then transmitted by the PBS, whereas the $|v\rangle$ photon is reflected by the PBS and the DM. The case shown in 2) is symmetric to the case in 1) but with the pump is vertically polarised and propagating anticlockwise inside the loop. In this case, the pair of photons exit the sagnac with opposite polarisation respect to the case in 1). The polarisation-entanglement between the two single photons is achieved when the input pump is in a superposition of horizontal and vertical light and the clockwise and anticlockwise paths are aligned to be perfectly collinear and indistinguishable. This can be appreciated in the bottom row with the panels a), b) and c) where one output of the sagnac is monitored with a camera. In a), the clockwise (pump H) and anticlockwise (pump V) path are clearly distinguishable. In b), they are improved in the horizontal direction by suitable beam-walking of the two mirrors in the sagnac. Finally in c) the two beams are made collinear.

is created by the crystal — is an entangled pair of the form:

$$|\Psi\rangle = \frac{|h\rangle|v\rangle + e^{i\phi}|v\rangle|h\rangle}{\sqrt{2}}, \tag{3.27}$$

with some phase ϕ depending on experimental factors. In Fig. 3.8 a picture of the source is shown together with a description of its working principle. In particular, the entanglement between the two single photons, arises from the indistinguishability of the two sagnac's internal loops (clockwise and anticlockwise). This kind of source can produce almost ideal Bell pairs if properly aligned, and throughout this thesis we assume the output of the interferometer to be

$$|\psi^-\rangle = \frac{|h\rangle|v\rangle - |v\rangle|h\rangle}{\sqrt{2}}. \tag{3.28}$$

The remaining Bell states $|\psi^+\rangle$, $|\phi^+\rangle$ and $|\phi^-\rangle$ can be obtained by single qubit rotations on one of the two photons.

3.6 Fusion Gate

Working with polarisation-encoded photons enables the scaling to multi-photon entangled states employing existing technology. The main optical component operating as a 2-qubit gate for photonic qubits is simply a polarisation beam splitter (PBS), which transmits only photons in the state $|h\rangle$ and reflects those in the state $|v\rangle$. This feature is exploited in the so-called type-I fusion gate, introduced in Ref. [47] to create a 3-qubit GHZ state entangled in polarisation out of two Bell pairs, with probability 1/2. Since then, this simple optical platform has been extensively used in all the multi-qubit experiments with single photons as those presented in this thesis.

To illustrate its working principle it is instructive to study within the quantum framework the basic scenario shown in Fig 3.9. Two single photons in the spatial modes m_1, m_2 are prepared in the state $|d\rangle_{m_1}|d\rangle_{m_2}$ where $|d\rangle$ is defined as $|d\rangle = (|h\rangle + |v\rangle)/\sqrt{2}$. They input a PBS which acts on the photons according to the

following mapping rules

$$|h\rangle_{m_1} \to |h\rangle_{m_1}, \quad |v\rangle_{m_1} \to i|v\rangle_{m_2}, \quad |h\rangle_{m_2} \to |h\rangle_{m_2}, \quad |v\rangle_{m_2} \to i|v\rangle_{m_1}. \tag{3.29}$$

Therefore it changes the spatial mode of a photon if its polarisation is vertical or leave it unchanged when the polarisation is horizontal. The phase i is a relative phase between the horizontal and vertical component, in this case assigned to the vector $|v\rangle$. The bipartite state after the action of the PBS in the Z-basis is given by

$$\frac{|h\rangle_{m_1}|h\rangle_{m_2} + i|h\rangle_{m_1}|v\rangle_{m_1} + i|h\rangle_{m_2}|v\rangle_{m_2} - |v\rangle_{m_1}|v\rangle_{m_2}}{2}. \tag{3.30}$$

We neglect the cases with two photons in the same spatial mode (which happens with probability 1/2), which experimentally is equivalent to post-select only the coincidence events between the detectors in the two modes. The renormalised state is entangled in polarisation

$$\frac{|h\rangle_{m_1}|h\rangle_{m_2} - |v\rangle_{m_1}|v\rangle_{m_2}}{\sqrt{2}}. \tag{3.31}$$

Physically, it is important to note that at the PBS the interaction of the photons generally involves all their degrees of freedom e.g. time or spectrum. Yet, without loss of generality, we assume that if the two photons are completely distinguishable in some degrees of freedom the bipartite system is described by the mixture

$$\frac{|hh\rangle\langle hh| + |vv\rangle\langle vv|}{2}. \tag{3.32}$$

Although the states in Eq. (3.31) and (3.32) give the same predictions in the Z-basis they differ in the X-basis where only the coherent pure state in Eq. (3.31) transforms as

$$\frac{|d\rangle_{m_1}|a\rangle_{m_2} + |a\rangle_{m_1}|d\rangle_{m_2}}{\sqrt{2}}, \tag{3.33}$$

whereas the mixed state in Eq. (3.32) will present all the components $|dd\rangle\langle dd|$, $|da\rangle\langle da|$, $|ad\rangle\langle ad|$, $|aa\rangle\langle aa|$ plus other coherence terms. Crucially, only the state in Eq. (3.33) will show interference fringes in a setup as in Fig 3.9, where one output is projected on $\langle d|_{m_1}$ and the other is varied from$\langle d|_{m_2}$ to $\langle a|_{m_2}$. From an experimental

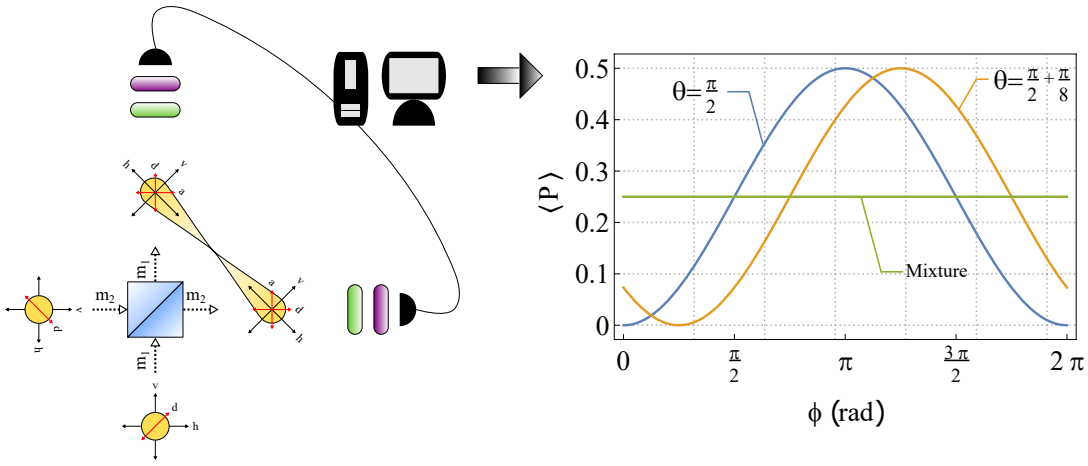


Figure 3.9: **Fusion gate and phase error.** Two single photons diagonally polarised are interfered at a PBS . If the interference successes the photons become entangled in polarisation showing interference fringes in the coincidences events. The phase of the experimental observed fringes (orange) might be shifted respect to the expected ones (blue) due to a lossy PBS used in the process. This error however can be easily fixed by rotating the reference frame of one of the two detection stages, by means of QWP (green) and HWP (purple).

point of view this phenomenon allows to verify whether the quantum interference at the PBS is correctly behaving, and so the fusion gate. If this is the case, it is easy to check that upon a detection of a photon in $\langle d|_{m_1}$ the fusion gate induces the transformation

$$FG_{\mathrm{I}} = \frac{1}{\sqrt{2}}\left(|h\rangle_{m_2}\langle h|_{m_2}\langle h|_{m_1} + |v\rangle_{m_2}\langle v|_{m_2}\langle v|_{m_1}\right). \tag{3.34}$$

Suppose now we prepare two Bell pairs, one in the spatial modes (m_1, a) whereas the second in (m_2, b). Then it is easy to see that the transformation in Eq. 3.34 and the detection of m_1 leaves the remaining three photons in an GHZ state in the modes a, b and m_2, hence transforming bipartite entanglement into tripartite one.

Depending on the experiment to be performed the fusion gate can be used in two different ways. If the graph state to be prepared should be heralded i.e. its presence in a given number of spatial modes is guaranteed by an heralding signal, then its implementation is the one explained in Sec 3.6, where one of the fusion gate's outputs is projected into $\langle d|$. This can be the case for example when after the generation of the graph states, 2-photon operations mixing the spatial modes of the photons are required. This will be the case in the experiment presented in Chapter 4. If instead no spatial mode mixing is required, but only local operations

on the graph states are performed, the heralding photon is not immediately detected and it is part of the graph state itself. The presence of the graph states in this case can only be guaranteed by post-selecting on N coincidence events, where N is the number of photons forming the graph states. This approach has the advantage of enabling the generation of larger graph states respect to the heralded case, and it will be used for the experiments in Chapter 5 and Chapter 6.

3.6.1 Experimental Tip

As a side note, directed to experimentalists dealing with this kind of setup, it should be mentioned that due to imperfections of any realistic PBS the state in Eq. (3.31) suffers a phase error reducing the quality of the interference if not corrected. One way to explain the problem is as follows: the transformations in (3.29) include a phase shift of $\pi/2$ between the polarisations of transmitted and reflected photons respectively, this phase factor can be justified within classical optics by imposing the conservation of energy of the transmitted and reflected fields in a lossless BS, as was shown by Degiorgio in 1979 [48]. In the conclusions of his short paper, he outlines how in lossy beam splitters the same conservation rule does not hold, and the phase shift might differ from the ideal $\pi/2$. Therefore, we replace the transformation rule $|v\rangle \rightarrow i|v\rangle$ for the reflected photons with the more general $|v\rangle \rightarrow e^{i\theta}|v\rangle$. Following the same procedure as above we get the entangled state

$$\frac{|h\rangle_{m_1}|h\rangle_{m_2} + e^{i2\theta}|v\rangle_{m_1}|v\rangle_{m_2}}{\sqrt{2}}. \tag{3.35}$$

The phase 2θ will not effect the statistic in the Z-basis but it will shift the interference fringes as shown in Fig 3.9 directly effecting the coherence and the quality of the 3-qubit GHZ. The phase can be easily corrected before any experiment by rotating the reference frame of the heralding measurement in the spatial mode m_1.

3.7 Graph States with a Photonic Platform

We have now all the ingredients to see how a graph state is realised in practice with a photonic platform. We note that in principle, to prepare any graph state experi-

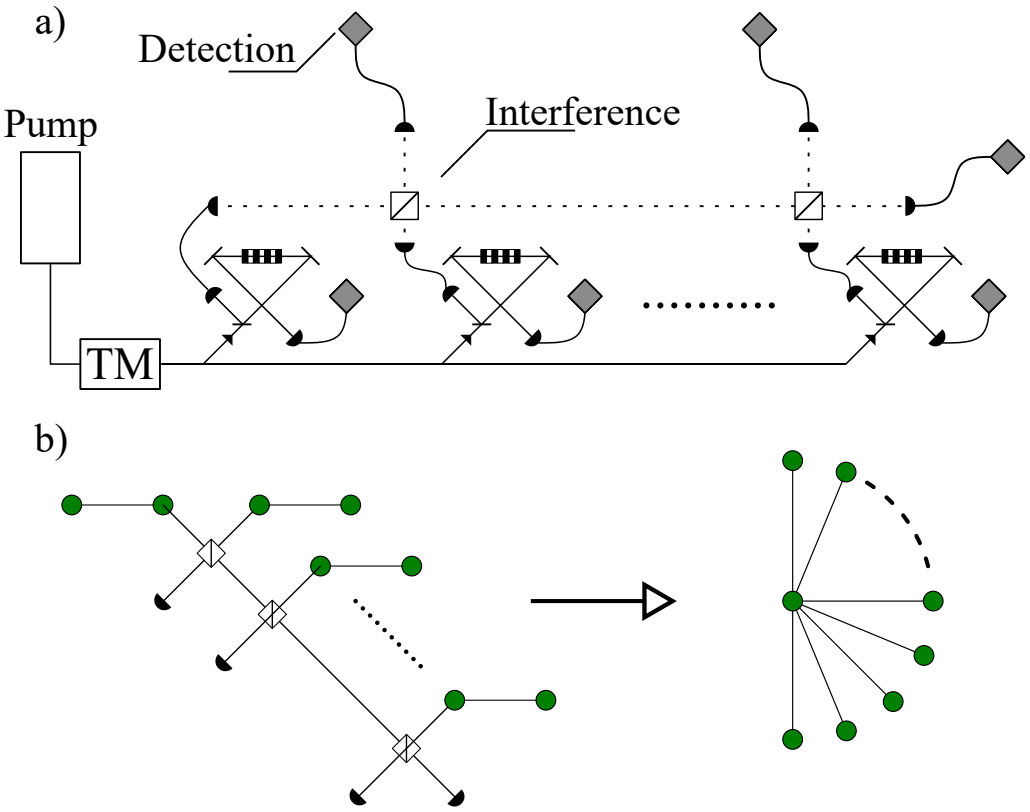


Figure 3.10: **Experimental generation of the n-photon star-graph. a)** A laser is temporally-multiplexed (TM) (see Sec 3.4) and it pumps n/2 polarisation-entanglement sources (see Sec 3.5) generating Bell pairs. One photon from each source is employed in a series of independent interferences and, after the successful detection of n photons a stabilizer state locally equivalent to the star-graph is obtained (see Sec. 2.4). **b)** The experimental scheme in a) is translated into the graph formalism.

mentally we would simply have to follow the prescription given in Sec. 2.4, that is to prepare each photon in the diagonal state $|d\rangle$ and apply a CZ gate between the connected vertices. While preparing single photons in the state $|d\rangle$ is straightforward, applying a CZ gate is not. To be more precise, an optical arrangement which can realise the CZ gate is known [49], however its probability of success is 1/9, which can be increased to 1/4 under specific scenarios [50]. It follows that when scaling to many photons, this approach is untenable. For this reason, the fusion gate with 1/2 probability of success presented in Sec. 3.6 is often preferred. For completeness we point out that also a type-II fusion gate can be defined. This is realised when both the outputs of the PBS are measured in the diagonal base. Thus, this type-II fusion gate consumes two qubits per fusion but it has the advantage of being more robust against losses and fusion's failure [47].

We remark that, in each of the chapters to follow we will see a detailed description of the experimental setup, specific to the experiment presented in that chapter. However to give the reader some intuition on how graph states are realised with a photonic setup we consider here a canonical example: the n-photon star-graph generation, see Fig. 3.10. The single photons for building the star-graph are generated with PPKTP crystals described in Sec. 3.1 and optimised for spectral purity (see Sec 3.2), heralding and brightness (see Sec. 3.3 and Sec. 3.4). The first step towards the generation of a n-photon star-graph is to create n/2 Bell pairs, this is achieved with the polarisation-entanglement source described in Sec 3.5. As shown in Fig 3.10a. the multi-photon graph state is built by interfering photons from different Bell pairs into a PBS, each interference realises a fusion gate as described in Sec 3.6. Following the scheme in Fig 3.10a., upon detection of n photons the following state is obtained:

$$|\mathrm{GHZ}_n\rangle = \frac{|h\rangle^{\otimes n} + |v\rangle^{\otimes n}}{\sqrt{2}}, \tag{3.36}$$

that is a n-photon GHZ state. This state is not properly a graph state in the sense that its stabilizers do not describe a graph, as explained in Sec. 2.4. However the n-photon GHZ state is a stabilizer state and therefore can always be mapped into a graph state by means of local Clifford operations as explained in Sec. 2.4. In particular, the state in Eq.(3.36) is equivalent to the star-graph in Fig 3.10b. up to one Hadamard gate on the external vertices. We note that the success probability for the n-qubit GHZ state is $1/2^n$, therefore it drops exponentially to 0 for increasing n, imposing an intrinsic limit on the scalability of this approach. So far, the largest star-graph was observed in Ref. [51] where a 12-photon state was generated with PDC sources. In their implementation the 12-photon coincidence rate was measured to be of $\approx 10^{-4}$ Hz and the fidelity of the state to be $F = 0.57$.

The star-graph or equivalently the GHZ state has been at the base of the majority of the photonic multi-photon experiments in the last 20 years or so. However, The GHZ state's hegemony in quantum information might come to an end in the future and other graph states could be required. With the setup of Fig. 3.10 some more different graphs could be realised as for example H-shaped graphs but a general framework to rigorously determine which graphs can be realised by the only means

of fusion gates and Bell pairs, is missing. An interesting work on this topic can be found in Ref. [52] where the accessible graph states with post-selection are obtained.

Chapter 4

Experimental Test of Local Observer-independence

In this chapter I present the story of an experiment. It shows that if you believe in quantum mechanics, locality, and freedom of choice then you shall give up the principle according to which facts are universal and objective, independent from the observer who established them. I start in Sec. 4.1 with a concise description of a well known conundrum affecting quantum scientists: the measurement problem. In Sec. 4.2, I move to the Wigner's friend thought experiment, fundamental to understand the scenario on which the experiment is presented. In Sec. 4.3, I briefly overview one more ingredient for the understanding of the experiment: the Bell's theorem. Finally, in Sec. 4.4 the experiment is described in detail from the setup to the results. I conclude in Sec. 4.5 and Sec. 4.6 with a discussion and on the conclusions drawn by the results.

I note that some of the text in this chapter is excerpted from the research paper in Ref. [53], where I led the experimental development of the project, from the characterisation and preparation of the full experimental setup to the data acquisition and data analysis.

4.1 The Measurement Problem

The modern formulation of the quantum theory is mainly due to contributions of Dirac and Von-Neumann [54, 55] and at its heart, we find the postulates on which

the theory stands [6]:

1. Any isolated physical system can be completely described by a state vector $|\psi\rangle$ in a Hilbert space.
2. The time evolution of the state of a closed quantum system is described by the Schroedinger equation according to the Hamiltonian H,

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle. \tag{4.1}$$

3. Quantum measurements are described by a set of measurement operators $\{M_m\}$ acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the system before the measurement is $|\psi\rangle$ then the outcome m is obtained with probability

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle, \tag{4.2}$$

and the state of the system after the measurement is

$$\frac{M_m|\psi\rangle}{\sqrt{p(m)}}. \tag{4.3}$$

Note that imposing $1 = \sum_m p(m)$ we set the condition $\sum_m M_m^\dagger M_m = \mathbb{1}$.

According to Postulate 1 quantum mechanics is universal, it can be applied to any isolated physical system whose state evolution can be described within the formalism. In fact, no restrictions on size, mass or other properties of the physical system are made. From Postulate 2, is follows that once the state of a closed system at time $t = 0$ is given, its evolution is always deterministic and reversible. Note that, from the linearity of the Schroedinger equation, it follows that a *superposition* of two solutions is itself a solution. Finally, Postulate 3 describes a special class of evolutions — the "measurements" — which follow a non-unitary rule whose prescription is to update the state of the system according to Eq. (4.3) conditioned on the probabilistic outcome which occurs with probability as in Eq. (4.2).

The presence in the formalism of two different evolutions, one unitary and deterministic as given by Postulate 2 and the other non-unitary and probabilistic as

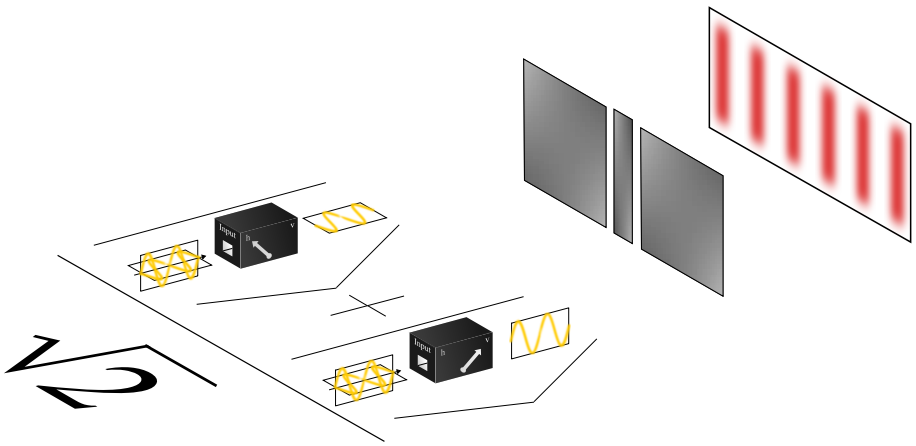


Figure 4.1: **The measurement problem.** According to quantum mechanics the measurement device is entangled with the single photon. If an interference experiment was performed by an external observer on the joint system, then an interference pattern would be observed as long as the position of the pointer remains unknown.

according to Postulate 3, is in essence the so-called measurement problem. In fact, no prescription is given on when to use one or the other, leading to an apparent contradiction. One could then think to drop either Postulate 1 or Postulate 2 to resolve the problem, however without the former we would not be able to explain the phenomenon of the quantum interference, without the latter we cannot account for definite single-value outcomes. This can be seen in the following exercise.

Consider a single photon whose horizontal and vertical polarisation states are described, according to the Postulate 1, by $|h\rangle$ and $|v\rangle$ respectively. Quantum mechanics allows, thanks to Postulate 2, to consider as a valid state the coherent superposition:

$$|d\rangle = \frac{|h\rangle + |v\rangle}{\sqrt{2}}. \tag{4.4}$$

Crucially, the state above is fundamentally different from the mixture

$$\mathbb{1} = \frac{|h\rangle\langle h| + |v\rangle\langle v|}{2}, \tag{4.5}$$

as can be verified by any interference experiment. Since quantum mechanics is postulated to be valid at any scale, the same argument holds for any physical system, like a measurement device. We consider for example a device which is able to interact with single photons and provided with a pointer, see Fig. 4.1. This device is initially in some state $|\text{ready}\rangle$ and the photon-device closed system is described

by the evolution:

$$|h\rangle|\text{ready}\rangle \rightarrow |h\rangle|\text{“pointer = h”}\rangle \tag{4.6}$$

$$|v\rangle|\text{ready}\rangle \rightarrow |v\rangle|\text{“pointer = v”}\rangle, \tag{4.7}$$

where $|\text{“pointer = h”}\rangle$ and $|\text{“pointer = v”}\rangle$ refer to the (macroscopic) states of the pointer physically pointing on the outcome h and v respectively. If the single photon prior to the interaction is prepared in a superposition (4.4) then according to the transformations (4.6) and (4.7):

$$\frac{|h\rangle + |v\rangle}{\sqrt{2}}|\text{ready}\rangle \rightarrow \frac{|h\rangle|\text{“pointer = h”}\rangle + |v\rangle|\text{“pointer = v”}\rangle}{\sqrt{2}}. \tag{4.8}$$

The joint system photon-device becomes entangled after the interaction. Therefore, it appears that the state of the device is definite only once the state of the photon is known too, and vice versa. This however might result in contrast with our experience; if we actually do such experiment we will always observe the pointer in a single and definite position, regardless our knowledge of the state of the photon. To reconcile theory with experimental observations, we can invoke Postulate 3 above. We just need to consider the interaction photon-device as a “measurement” i.e. a non-unitary and probabilistic evolution described by equation Eq. (4.3) rather than Eq. (4.1). If so, the state's description given in (4.8) does not hold and it should be replaced by:

$$p(\text{“outcome is h”}) = 1/2 \rightarrow |h\rangle|\text{“pointer = h”}, \rangle \tag{4.9}$$

$$p(\text{“outcome is v”}) = 1/2 \rightarrow |v\rangle|\text{“pointer = v”}\rangle. \tag{4.10}$$

Depending on the outcome, the photon-device state is updated accordingly. This process is sometimes known as “collapse of the wave function” and whether is merely a mathematical tool or an actual physical process is still under debate [56].

Nevertheless, for all practical purposes [57], quantum mechanics formalism with the three postulates above is one of the most successful theories in predicting experimental results. However, it is clear that the problem remains.

When facing these problems, the boundary between metaphysics and physics might become blurry [58]. However, is notable the effort made so far by the scientific community to either assign a metaphysical meaning to the formalism as it is, or modifying it to obtain a new theory able to pass both real and thought experiments. In this vein, many interpretations of quantum mechanics have arisen.

Historically, the first interpretation of quantum mechanics is known under the name of the Copenhagen interpretation. A unique "manifesto" of the interpretation does not exist but it is rather a collection of contributions from 1925 to 1927 due to the pioneers of the theory such as Niels Bohr and Werner Heisenberg[1]. The Copenhagen interpretation focuses on the metaphysics of the wave function, which is believed to give a *complete* description of the physical system the wave function is assigned to. In particular before any measurement, the wave function is merely a mathematical tool, it is a state of knowledge (epistemic) rather than a state of reality (ontic). Only after a measurement, the knowledge of the observer is updated and the wave function collapsed. The boundary separating the pre-measurement and post-measurement description is the so-called Heisenberg cut. The main critique to the interpretation is that no prescription is given for how to locate such cut and that observers have to be considered as external entities, not described by the quantum theory.

This view of the quantum formalisms found a first opposition in 1927 when Louise De Broglie [59] with a contribution at the famous Solvay Congress, suggested the possibility of completing quantum theory by adding a new equation describing the motion of particles in time. This guiding equation could not be solved without knowing the form of the particles' wave function, in turn obtained by solving the Schroedinger equation. De Broglie never formalised his ideas and he lately became a supporter of the Copenhagen interpretation. However in 1952 David Bohm rediscovered that theory, today known as Bohmian mechanics [60]. In particular, given any physical system, its initial configuration is randomly distributed according to $|\psi|^2$ and its evolution, given by solving the guiding equation, is fully deterministic. Within this formalism observers have no special role as they are only other physical systems. The main criticism to the theory is that it is sometimes simply considered

[1]It might be more accurate to call this ensemble of contributions, the Copenhagen interpretations.

as a reformulation of quantum mechanics with superfluous complexity introduced by the guiding equation.

Another important interpretation of quantum mechanics is the Hugh Everett "relative state" formulation of quantum mechanics [61, 62]. Everett published his view of quantum mechanics in his Ph.D. thesis[2] before leaving academia and his research activity. Everett's idea is quite simple, if the measurement problem comes from the existence of two incompatible dynamics within the same formalism, then the solution is to only use one of them. In particular, Everett's proposal was to drop the collapse postulate from the standard formulation of quantum mechanics then deduce the empirical predictions of the standard theory as the subjective experiences of observers. More recently, Everett's theory was embedded with the decoherence theory evolving in the so-called many-worlds interpretation [63, 64].

One more approach to face the measurement problem is to make the Schrödinger equation non-linear, as supported by the family of the collapse theories [65, 66]. These theories add a stochastic term to the Schrödinger equation causing the collapse of the wave function when the system described has a given size or mass. For this reason, these theories can be experimentally tested by observing quantum effects for bigger and bigger systems.

In this thesis, the reader will not find a solution of the measurement problem. However an insight on the observations and observers in quantum mechanics will be given.

4.2 The Wigner's Friend Thought Experiment

Imagine a closed laboratory where a single photon in the superposition state (4.4) is measured by an observer, Wigner's friend, see Fig. 4.2. Outside, Wigner, describes the joint photon-friend system as a closed quantum system evolving according to the Schrödinger equation. Following exactly the same arguments as in the previous section, Wigner will describe the joint system as an entangled quantum state given by:

$$\frac{|h\rangle + |v\rangle}{\sqrt{2}}|\text{ready}\rangle \rightarrow \frac{|h\rangle|\text{I see h}\rangle + |v\rangle|\text{I see v}\rangle}{\sqrt{2}}, \tag{4.11}$$

[2]No new interpretations of quantum mechanics will be found in this Ph.D. thesis, unfortunately.

where the states $|\text{I see h}\rangle$ and $|\text{I see v}\rangle$ are referred to Wigner's friend having observed the measurement device in the state $|\text{“pointer = h”}\rangle$ and $|\text{“pointer = v”}\rangle$ respectively. Thus, they describe the physical system of the friend having experienced a definite and unique outcome. Wigner pointed out that the state in equation (4.11) is indeed correct according to quantum mechanics but, does not account for the friend inside having observed a definite outcome. Wigner, however, presuming that a conscious being must always be in a definite state, concludes that albeit the macroscopic states $|\text{I see h}\rangle$ and $|\text{I see v}\rangle$ are valid, the equation (4.11) is not. In particular, he suggests that Postulate 3—the measurement postulate—should be applied whenever a conscious observer is included in the quantum description. With this additional rule, the measurement problem fades away, equation (4.11) is updated to either $|h\rangle|\text{I see h}\rangle$ or $|v\rangle|\text{I see v}\rangle$ even if Wigner does not know which one of the two.

When in 1961 Eugene Wigner proposed his thought experiment [67] his interest was philosophical rather than scientific. In fact, he leveraged on the measurement problem to jeopardize the philosophy of materialism, which asserts that everything including consciousness can be described by science. Wigner's claim is that if quantum mechanics is applied to human beings[3] then it simply fails to describe the observer's experience. In this thesis no arguments involving consciousness are invoked, however, the thought scenario proposed by Wigner will be.

Following Wigner's work, his scenario has been often a test-bed for the various interpretations of quantum mechanics. For instance, 24 years later, David Deutsch compared the canonical Copenhagen interpretation with Everett's relative state formulation [61] in a twist of the Wigner's friend scenario [68]. He considers an additional step after the friend's measurement, who upon the observation of the measurement's outcome (either h or v) writes on a piece of paper the following statement “I see a definite outcome” and sends it to Wigner. This simple prescription is very important in fact, as long as the actual value of the outcome is not revealed, the description from Wigner's perspective does not change. Wigner now has to acknowledge that the friend inside the lab has experienced a unique and definite outcome, however if Wigner now performs an interference measurement on the joint photon-

[3]Albeit a definition of consciousness is not given by Wigner, if such definition exists then any human being should satisfy it.

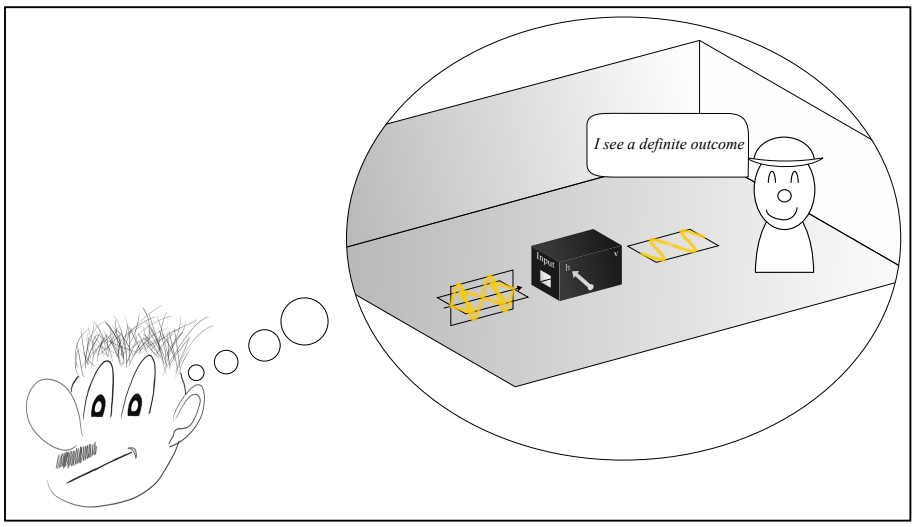


Figure 4.2: **Wigner's friend thought experiment.** Wigner's friend is inside a closed lab where the measurement of a photon's polarisation is performed, and a definite outcome observed. Wigner does not have direct access to the laboratory and from his perspective the friend's interaction with the photon leave the closed system entangled, therefore in contradiction with the friend's experience.

friend system, he can verify that the state assignment in Eq. (4.11) is indeed correct. The facts established by Wigner and his friend are incompatible with the predictions of quantum mechanics. Deutsch's conclusion is that the Copenhagen interpretation fails in describing such incompatibility whereas Everett's interpretation does not. In the following, with the Wigner's friend scenario, we will refer to Deutsch's extension. In fact, beside the debate on the interpretations of quantum mechanics, such scenario will allow us to unveil new interesting insights. What we will show is how quantum mechanics might be incompatible with observer-independent facts, where with the term "fact" we refer to the realisation of a measurement outcome being a piece of information stored in some memory (similarly to the piece of paper in the thought experiment).

Before diving into a modern reformulation of the Wigner's friend scenario and the experimental implementation, we need to review one more fundamental result in quantum theory i.e. the Bell's theorem.

4.3 Bell's Theorem

In the early 1960s, John Stewart Bell published [69] one of the most influential papers of the modern understanding of quantum mechanics foundations. Bell's aim

was to tackle in a simple and elegant way the notorious 1935 Einstein-Podolsky-Rosen (EPR) paradox [70].

The EPR argument is structured as follow. The authors first postulate that if, without in any way disturbing a system, we can predict with certainty (i.e.,with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity. Then they consider a pair of entangled particles in the singlet state and space-like separated. Since according to quantum mechanics we can predict with certainty the result of a measurement (for example of a spin component) on particle 1 by previously measuring the same observable on particle 2, the outcome measured on particle 1 is an element of physical reality according to the postulate above. However, as the particles are space-like separated the outcome of the measurement on particle 1 could not be causally influenced by the measurement's setting on particle 2 (locality assumption). This implies that the value of the outcome must be predetermined (predetermination assumption). Since within the quantum formalism the result of an individual measurement is not predetermined, it follows that quantum mechanics can not be a complete theory but should be supplemented by additional variables. The role of the hidden variables is therefore to make measurement outcomes predetermined, which is the claim of the EPR argument. Historically, the EPR argument was proposed using particles entangled in position-momentum, leading to a contradiction with the Heisenberg uncertainty principle. This was then reformulated with $1/2-$spin particles by Bohm [60].

Following the EPR paper, Bohr replied in the same year [71] to defend his position aligned with the Copenhagen interpretation according which quantum mechanics is already complete. His claim was that the EPR argument does not apply to quantum mechanics where elements of reality do not exist until measured. To make the debate even more exciting, the well-known mathematician Von Neumann [54] claimed that he had proven Einstein's dream of a deterministic reformulation of quantum theory to be mathematically impossible, a hidden-variable theory can not exist.

Bell's theorem eventually dispelled the dense fog covering quantum mechanics. He proved that contrary to the Von Neumann's claim, a hidden-variable theory giv-

ing the same predictions of quantum theory but restoring the deterministic character of classical physics, can exist but must be non-local i.e. the results of a measurement on one system are affected by operations on a distant system, however remote.

Ten years later, Bell published a new manuscript [72] reformulating his theorem in terms of the notion of local causality i.e. the results of a measurement on one system are not causally influenced by either the measurement setting or the measurement outcome of a measurement on a space-like separated system. Quantum mechanics is not compatible with the single assumption of local causality [72]. For a discussion on the differences and similarities of the notions of locality and local causality, the reader is pointed to Ref. [73].

In the following we report more in detail the Bell's theorem, using a reformulation due to Clauser, Horne, Shimony and Holt [74, 75]. Consider two distant observers Alice and Bob sharing a pair of photons in some state $|\psi\rangle$. Alice measures an observable relative to some setting x on her system obtaining an outcome a, similarly Bob measures an observable y on his system obtaining the outcome b. In general x, y can be randomly chosen within some set of possible measurements $x \in \{x_0, x_1, x_2, ..\}$ and $y \in \{y_0, y_1, y_2, ..\}$ and each measurement can lead to different outcomes $a \in \{a_0, a_1, a_2, ..\}$ and $b \in \{b_0, b_1, b_2, ..\}$. The outcomes are therefore governed by some probability distribution $p(a, b|x, y)$ which could for example be estimated by repeating the experiment many times. In absence of correlations the observers will find that

$$p(a, b|x, y) = p(a|x)p(b|y). \tag{4.12}$$

However if the states $|\psi\rangle$ employed in the experiment are entangled they could observe

$$p(a, b|x, y) \neq p(a|x)p(b|y). \tag{4.13}$$

The presence of correlations should not surprise the two observers. In fact, the two photons might have interacted in the past conditioning the outcome of the experiment. In particular, there might be some variables λ having a joint causal influence on both outcomes fully accounting for the correlations between them. Formally, we can consider a model going beyond quantum mechanics and accounting for the correlations observed by Alice and Bob. In particular, we consider a model with the

following assumptions

$$p(a|x,y,b,\lambda) = p(a|x,\lambda), \tag{4.14}$$

$$p(b|y,x,a,\lambda) = p(b|y,\lambda), \tag{4.15}$$

$$q(\lambda|x,y) = q(\lambda). \tag{4.16}$$

Equations (4.14) and (4.15) express the notion of locality (or local causality according to Ref. [73]) stating that the outcomes a, b only causally depend from the *local* measurement setting and the variables λ. Whereas Eq. (4.16) known as freedom of choice (FOC) assumption rules out any dependence of λ on the choice of the measurement settings (see Fig. 4.3). If we further assume that λ are distributed according to some function $q(\lambda)$ well-defined for every value of λ, we can write a condition for the observed probability distribution $p(a,b|x,y)$

$$p(a,b|x,y) = \int_\lambda d\lambda\, p(a|x,\lambda)p(b|y,\lambda)q(\lambda). \tag{4.17}$$

The models for which the $p(a,b|x,y)$ can be decomposed as in Eq. (4.17) are called local hidden variable (LHV) models. Therefore, in an experimental scenario, Alice and Bob can collect statistics by repeating the experiment described above, and approximate the probability distribution $p(a,b|x,y)$ with some given confidence. If $p(a,b|x,y)$ can not be decomposed as in Eq. (4.17), then the observed data can not be explained by a LHV model.

To see how quantum theory predictions do not admit the decompositions of Eq. (4.17) we consider $x \in \{x_0, x_1\}$, $y \in \{y_0, y_1\}$ and $a, b \in \{-1, +1\}$. We consider the expectation values $\langle a_x b_y\rangle = \sum_{a,b} ab\, p(a,b|x,y) = \int_\lambda d\lambda\, q(\lambda)\langle a_x\rangle_\lambda \langle b_y\rangle_\lambda$ where

$$\langle a_x\rangle_\lambda = \sum_a a\, p(a|x,\lambda), \tag{4.18}$$

$$\langle b_y\rangle_\lambda = \sum_b b\, p(b|y,\lambda), \tag{4.19}$$

where $\langle a_x\rangle_\lambda$ and $\langle b_y\rangle_\lambda$ take values in $[0,1]$. It can be shown that, if $p(a,b|x,y)$ can

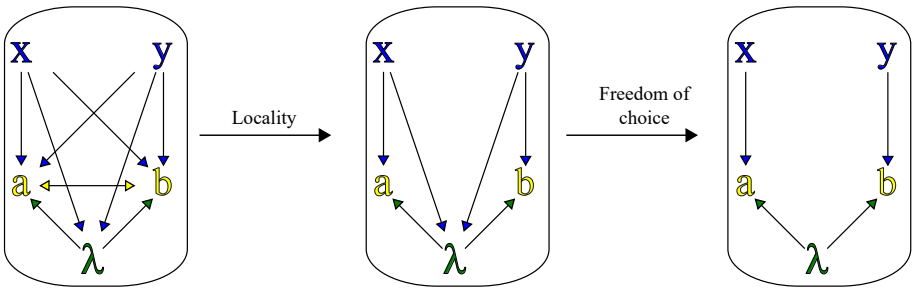


Figure 4.3: **Bell non-locality.** It is sometimes instructive to picture the causal structure of a Bell scenario with a directed acyclic graph. The nodes are either the measurement settings (in blue) the outcomes (in yellow) and the hidden variables λ (in green). Nodes are connected by arrows whose direction is from the cause to the effect. In the figure from the left to right a general causal network is shown, then with the locality assumption applied and finally with the freedom of choice assumption. The resulting structure leads to Eq. (4.17).

be decomposed as in Eq. (4.17), the so-called CHSH inequality

$$S = \langle a_0 b_0 \rangle + \langle a_0 b_1 \rangle + \langle a_1 b_0 \rangle - \langle a_1 b_1 \rangle \leq 2, \tag{4.20}$$

must be satisfied. Upon opportune choice of x, y and when Alice and Bob share a maximally entangled state, quantum mechanics predicts $S = 2\sqrt{2}$ thus violating the CHSH inequality (4.20). Hence, quantum mechanics predictions can not comply with any local hidden variable theory, which is the essence of Bell's theorem.

The first experimental Bell test was performed with single photons in 1972 by Freedman and Clauser [76] then with improved statistical accuracy 10 years later by Aspect, Grangier and Roger [77, 78]. After these precursor experiments, the CHSH inequality was violated within more and more standard deviations thanks to the improvements in quantum optics and on the quality of single photons sources. However, it was lately pointed out that such violations suffered of possible loopholes deriving from experimental limitations such as limited efficiency of detectors and losses in the experimental setup. Before moving to the main section of this chapter on the Bell-Wigner test, we review in the following the detection and locality loopholes as similar loopholes will emerge in light of the new Bell-Wigner test.

4.3.1 Detection Loophole

The detection loophole is due to presence of losses between the source and the detection stage in addition to detectors with non-unit efficiency, leading to some overall effective transmission $\eta < 1$. If a finite number of photons is created at the source, only a sample of those photons will be eventually employed for the evaluation of the CHSH inequality (4.20). In this regard it was pointed out [79, 80] that any experimental violation of the inequality must account the additional "fair sampling" assumption, stating that the sample considered should be statistically representative of the all possible events, including those where a photon was not detected. This additional assumption can be dropped only if η is higher than some threshold η^*. In particular for $\eta < \eta^*$ is possible to construct LHV models producing the observed data [79, 80], opening the detection loophole. The standard approach to compute the threshold η^* is to use the Clauser-Horne (CH) inequality [79] rather than the CHSH inequality in Eq. (4.20) and considering the no-click events as an additional outcome 0 and merge them to one of the two valid outcomes ± 1. For two parties sharing a two-qubit maximally entangled state and dichotomies measurements the probability that both detectors click is η^2 whose outcomes result in the maximal violation $2\sqrt{2}$. If only one detector does not click (outcome 0) the corresponding value of S is 0. Finally, if both detectors do not click with probability $(1-\eta)^2$ the classically correlated outcome leads to $S = 2$. Therefore the data is statistically significant if

$$2\sqrt{2}\,\eta^2 + 2(1-\eta)^2 > 2 \tag{4.21}$$

which is satisfied for $\eta > \eta^* = \frac{2}{1+\sqrt{2}} \approx 82.8\%$. Due to losses and limited detection efficiencies, this condition can be very limiting for optical systems making other platforms as atoms more suitable for a detection loophole-free Bell experiment.

Experimentally, the first violation of the inequality free from the detection loophole was performed in 2001 employing two entangled trapped ions [81]. The detection loophole was then lately closed using single photons in 2013 [82].

4.3.2 Locality Loophole

To comply with the assumptions made on deriving the decomposition in Eq. (4.17) the experimental setup should be such that the measurement sites are space-like separated and the measurement settings should not be correlated with the hidden-variable λ, satisfying the locality assumption in Eq (4.14) and Eq (4.15), and the FOC assumption in Eq. (4.16). The locality loophole is opened when at least one of the locality assumptions is not met[4], whereas the freedom of choice loophole is opened when the FOC assumption is not met.

The locality assumptions can be satisfied by spatially locating the sites such that the measurement duration (given by the time required from the setting preparation to the outcome evaluation) is shorter than the time taken for a signal travelling at the speed of light to reach the other site.

The FOC assumption instead, is satisfied if the measurement settings are chosen randomly and freely. These two last propositions are however not well defined and might lead to a situation where the freedom of choice loophole can not be intrinsically closed. In fact, the random choice is based on the notion of randomness which is a controversial concept per se (see Ref. [83] for a debate on randomness and chance in philosophy and science). For example, an event believed to be genuinely random within quantum mechanics might then be revealed as deterministic in some other theory.

Similarly, for the locality requirement, the absence of some sort of superdeterminism governing a priori all the outcomes of any measurements, can not be disproved by definition.

Nevertheless, in the last 10 years technology was pushed to the edge in order to close the locality and detection loophole simultaneously, leading in 2015 to three independent experiments achieving a loophole-free Bell test [84–86].

Finally, it is worth to mention a recent locality test where light emitted from two quasars at a distance of eight billion light years, was used to select the measurement settings of the Bell test [87].

Loophole-free Bell tests embody the advances in experimental quantum mechan-

[4]One could argue that any experiment failing the locality assumptions is not a Bell test in the first place.

ics, effecting technologies such as quantum key distribution. What is next, is not easy to envision. However, new challenges might be revealed by a new fundamental test: the Bell-Wigner test, presented in the following section.

4.4 A Bell-Wigner Test

In this section I finally present the main topic of this chapter, the experimental results of the first Bell-Wigner test [53]. The experiment is based on the theory recently developed by Brukner [88, 89] built upon the principles of both the Wigner's friend scenario and the Bell's theorem. In the following I will use the same formalism as in Ref. [53].

4.4.1 Two Irreconcilable Facts

Recalling the concepts introduced in Sec 4.1 and Sec 4.2, consider a closed lab where a single photon is measured by an observer (Wigner's friend), using some device able to interact with the photon and distinguish two orthogonal polarisations, $|h\rangle$ and $|v\rangle$. After the measurement is performed, the outcome is stored by the observer in a memory which therefore can either be in the state $|\text{“photon is } h\text{”}\rangle$ or $|\text{“photon is } v\text{”}\rangle$. We stress that here the measurement outcome stored in the memory, is a fact i.e. a piece of classical information. After the measurement is realised, the friend sends a signal to the observer outside (Wigner) encoding the statement “I see a definite outcome” as in the Deutsch's extension of the Wigner's friend experiment [68]. As long as the signal does not contain any information about the outcome's value, it does not change the description from Wigner's perspective. In fact, according to quantum mechanics, the state of the joint system photon-memory-signal is:

$$\frac{\big(|h\rangle|\text{“photon is } h\text{”}\rangle + |v\rangle|\text{“photon is } v\text{”}\rangle\big)|\text{I see a definite outcome}\rangle}{\sqrt{2}}. \tag{4.22}$$

As the state of the signal factorises with that of the photon-memory, from the Wigner's perspective the photon and the memory are still entangled. We note that here the memory plays an equivalent role of the friend in the standard Wigner thought experiment in Sec 4.2. Furthermore, we note that here as in the Deutsch's

extension of the Wigner's friend experiment the signal plays a crucial role. In fact, Wigner must now acknowledge that the friend inside the lab has indeed observed a definite outcome, whose value is registered into the memory. Concurrently, Wigner can in principle verify his state assignment with an interference measurement on the joint system. If, as predicted by quantum mechanics, he observes interference then he has established the fact: "my friend's memory and the photon are entangled". The friend's fact and the Wigner's fact appear to be contradictory, but yet simultaneously real. We ask if these facts are objective and independent from the observer who established them. The key idea from Brukner is to put into test whether these two facts can be reconciled in a theoretical framework, possibly beyond quantum mechanics, where the two facts can be jointly assigned a truth value and therefore being objective observer-independent facts. This question can be addressed formally, by considering an extension of the Wigner's friend scenario described in the following section.

4.4.2 No-go Theorem for Observer Independent Facts

Consider a pair of entangled photons, shared between two separate laboratories controlled by Alice and Bob, respectively see Fig. 4.4. Inside these laboratories, Alice's friend and Bob's friend measure their respective system non-destructively and record the outcomes in some memory. Outside the laboratories, in each run of the experiment, Alice and Bob can choose to either measure the state of their friend's record—i.e. to attest the "facts" established by their friend; or to jointly measure the friend's record and the system held by the friend—to establish their own "facts". In the first case they measure the observables A_0 (for Alice's friend) and B_0 (for Bob's friend) defined as

$$A_0 = B_0 = \mathbb{1} \otimes \big(|\text{“photon is } h\text{”}\rangle\langle\text{“photon is } h\text{”}| - |\text{“photon is } v\text{”}\rangle\langle\text{“photon is } v\text{”}| \big), \tag{4.23}$$

In the second case instead, they measure the observables A_1 (for Alice) and B_1 (for Bob) which are defined as

$$A_1 = B_1 = |\Phi^+_{\text{photon/record}}\rangle\langle\Phi^+_{\text{photon/record}}| - |\Phi^-_{\text{photon/record}}\rangle\langle\Phi^-_{\text{photon/record}}|,$$

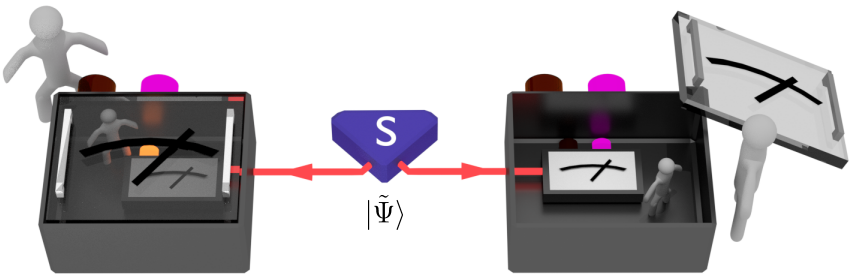


Figure 4.4: **Extended Wigner's friend experiment.** We consider an extended version of the Wigner's friend experiment. An entangled state is sent to two different laboratories, each involving an experimenter Alice's friend (Bob's friend) measuring the polarisation of the incoming single photon, whose value is recorded in her (his) memory. Outside, Alice (Bob) either measures the closed system in some entanglement base or observes the outcome of the friend's measurement by opening the lab.

where $|\Phi^{\pm}_{\text{photon/record}}\rangle = (|hh\rangle \pm |vv\rangle)/\sqrt{2}$. Note that in principle observables A_1 and B_1 have four eigenstates, however as explained in the following two of them have a zero eigenvalue and omitted above. After comparing their results, Alice and Bob can estimate the probability distributions $P(A_x, B_y)$ for all four combinations of $x, y = 0, 1$. As outlined above, the facts A_1, B_1 attributed to Alice and Bob and A_0, B_0 attributed to their friends' measurements may be inconsistent.

We assume that one can jointly assign truth values to the fact's A_1, A_0 (B_1, B_0) as described by the joint probability distribution $P(A_0 = \pm 1, A_1 = \pm 1)$ $(P(B_0 = \pm 1, B_1 = \pm 1))$, with the truth value "true" corresponding to the outcome $+1$ and "false" to -1. We shall call this assumption O, *observer-independent facts*, stating that a record or piece of information obtained from a measurement should be a "fact of the world" that all observers can agree on—and that such "facts" take definite values even if not all are "co-measured" [89]. We further assume *locality* (L) stating that Alice and Bob measurement choices do not influence each others' outcome,

$$P(A_0 = \pm 1, A_1 = \pm 1 | B_0, B_1) = P(A_0 = \pm 1, A_1 = \pm 1), \tag{4.24}$$

$$P(B_0 = \pm 1, B_1 = \pm 1 | A_0, A_1) = P(B_0 = \pm 1, B_1 = \pm 1), \tag{4.25}$$

and *freedom of choice* (F) assuming that Alice and Bob can freely choose their measurements A_0, A_1 and B_0, B_1, it should then be possible to construct a single

probability distribution $P(A_0, A_1, B_0, B_1)$ for the four individual facts under consideration, see Sec 4.3 for a more details on the notion of L and F.

Any joint probability distribution satisfying these assumptions must then satisfy Bell inequalities [90]. More specifically, when the variables A_x, B_y take values $a, b \in \{-1, +1\}$, then the average values $\langle A_x B_y \rangle = \sum_{a,b} abP(A_x = a, B_y = b)$ must obey the Clauser-Horne-Shimony-Holt inequality [74] (see Sec 4.3):

$$S = \langle A_1 B_1 \rangle + \langle A_1 B_0 \rangle + \langle A_0 B_1 \rangle - \langle A_0 B_0 \rangle \leq 2. \tag{4.26}$$

As shown in Refs. [88, 89], a violation of the inequality above is, however, possible in a physical world described by quantum theory. Such a violation would demonstrate that the observed probability distributions $P(A_x, B_y)$ are incompatible with assumptions F, L, and O. Therefore, if we accept F and L, it follows that the pieces of information corresponding to facts established by Alice, Bob, and their friends cannot coexist within a single, observer-independent framework [88, 89]. Notably this is the case even though Alice and Bob can acknowledge the occurrence of a definite outcome in their friend's closed laboratory.

We note that, although Bell's mathematical machinery [91] (see Sec 4.3) is used to show the result, the set of assumptions considered here—and therefore the conclusions that can be drawn from a violation of inequality (4.26)—are different from those in standard Bell tests. In fact, while they share assumptions L and F, the third assumption of predetermination (PD) in the original Bell theorem [69], for instance, differs from our assumption O in that it is only concerned with the deterministic (or otherwise) nature of measurement outcomes, not with their objectivity as in O. A Bell test is indifferent to the observables used and the underlying system, such that any violation suffices to rule out the conjunction of L, F and PD. In contrast, a Bell-Wigner test is based on very specific observables that satisfy the definition of an observation given below and thus represent facts relative to different observers.

4.4.3 Observer or Agent?

Before moving to the experimental details, let us first clarify our notion of an observer. Formally, an observation is the act of extracting and storing information

about an observed system. Accordingly, we define an observer as follows

Definition 4.1 (Observer)
An observer is any physical system that can extract information from another system by means of some interaction, and store that information in a physical memory.

According to this definition, all we require from an observer is the capability of extracting and storing information. We note that this definition covers large (even conscious) observers such as humans, as well as measurement devices independently from their sizes. As long as the physical system chosen to be an observer satisfies the definition above, it is able to establish "facts", therefore can play the roles of Alice's friend and Bob's friends in a Bell-Wigner test. Alice and Bob however, have an additional requirement, that is to compute the expectation values in (4.26). We define an agent as follow

Definition 4.2 (Agent)
An agent is any physical system that can extract information from another system by means of some interaction, store that information in a physical memory and process that information.

An agent, after the extraction of the information should be able to use it. For example, Alice and Bob in the Bell-Wigner test compute the value of an inequality (4.26), hence they are agents. A mere observer is not capable of this according to our minimal definition.

4.4.4 Experimental Protocol

Bearing in mind the extended Wigner's friend scenario sketched in 4.4 and the definition of observer, in the following is presented the experimental protocol realising the Bell-Wigner test. As in figure 4.5, the building blocks are: three sources of entangled photons S_0, S_A and S_B; two fusion gates (see Sec 3.1 for details) employed by the friends to establish their facts; two Bell measurements employed by Alice and Bob to verify their state assignment.

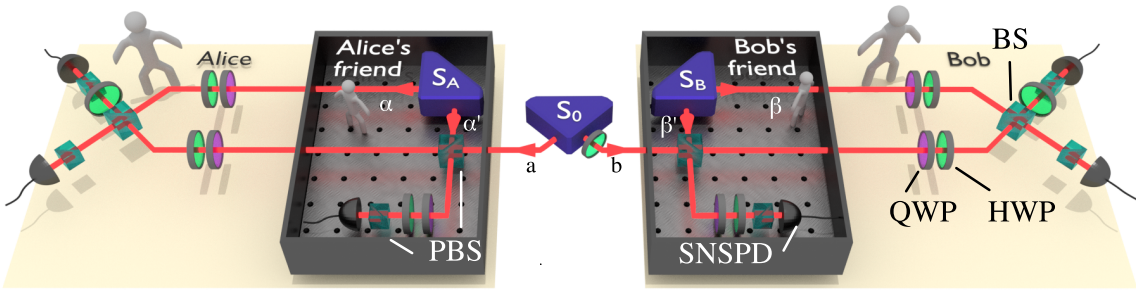


Figure 4.5: **Experimental scenario.** Pairs of entangled photons from the source S_0, in modes a and b, respectively, are distributed to Alice and Bob's friends, who locally measure their respective photon in the h, v basis using entangled sources S_A, S_B and type-I fusion gates. These use nonclassical interference on a polarising beam splitter (PBS) together with a set of half-wave (HWP) and quarter-wave plate (QWP). The photons in modes α' and β' are detected using superconducting nanowire single photon detectors (SNSPD) to herald the successful measurement, while the photons in modes α and β record the friends' measurement results. Alice (Bob) then either performs a Bell-state measurement via non-classical interference on a 50/50 beam splitter (BS) on modes a and α (b and β) to measure A_1 (B_1) and establish her (his) own fact, or removes the BS to measure A_0 (B_0), to infer the fact recorded by their respective friend.

Initialisation. Source S_0, initially prepared in the $|\psi^-\rangle$ state, is rotated to,

$$\begin{aligned} |\widetilde{\Psi}\rangle_{ab} &= \mathbb{1} \otimes U_{\frac{7\pi}{16}} |\Psi^-\rangle_{ab} = \\ &= \frac{1}{\sqrt{2}} \cos\frac{\pi}{8} \left(|h\rangle_a|v\rangle_b + |v\rangle_a|h\rangle_b\right) + \frac{1}{\sqrt{2}} \sin\frac{\pi}{8} \left(|h\rangle_a|h\rangle_b - |v\rangle_a|v\rangle_b\right). \end{aligned} \tag{4.27}$$

using a half-wave plate on its right output arm at an angle $7\pi/16$, given by $U_{\frac{7\pi}{16}} = \cos(\frac{7\pi}{8})\,\sigma_z + \sin(\frac{7\pi}{8})\,\sigma_x$ (where $\mathbb{1}$ is the identity, σ_z, σ_x are the Pauli operators). This state maximises the violation of inequality (4.26) for our choice of measurement settings. This photon pair is distributed to the laboratories of Alice's friend and Bob's friend.

Alice's friend observation. Source S_A is prepared in the state $|\Psi^-\rangle_{\alpha'\alpha}$. The photonic Alice's friend in the mode α' measures non-destructively, the polarisation of the incoming photon in the mode a. This is done by means of a type-I fusion gate [47], described by the transformation:

$$FG_{\mathrm{I}} = \frac{1}{\sqrt{2}}\left(|h\rangle_a\langle h|_a\langle h|_{\alpha'} - |v\rangle_a\langle v|_a\langle v|_{\alpha'}\right), \tag{4.28}$$

where a and α' are the PBS's input modes, and a is the output mode (we keep the

names of the input and output modes a the same for simplicity). The other output mode α' is measured to herald the success of the operation, which happens with probability of $\frac{1}{2}$. We note that the click of the heralding detector does not contain any information about the polarisation of the observed photon. However, it serves to mark that a definite outcome was observed and a fact established. The role of the detector measuring the mode α' is therefore equivalent to the piece of paper in the Deutsch's extension of the original Wigner's friend experiment.

Depending on the state of the incoming photon, the operation performed by Alice's friend transforms the overall state as

$$\begin{aligned} |h\rangle_a|\Psi^-\rangle_{\alpha'\alpha} &= \frac{1}{\sqrt{2}}\big(|h\rangle_a|h\rangle_{\alpha'}|v\rangle_\alpha - |h\rangle_a|v\rangle_{\alpha'}|h\rangle_\alpha\big) \xrightarrow{FG_{\mathrm{I}}} \frac{1}{2}|h\rangle_a|v\rangle_\alpha, \\ |v\rangle_a|\Psi^-\rangle_{\alpha'\alpha} &= \frac{1}{\sqrt{2}}\big(|v\rangle_a|h\rangle_{\alpha'}|v\rangle_\alpha - |v\rangle_a|v\rangle_{\alpha'}|h\rangle_\alpha\big) \xrightarrow{FG_{\mathrm{I}}} \frac{1}{2}|v\rangle_a|h\rangle_\alpha. \end{aligned} \tag{4.29}$$

Hence, the state $|h\rangle_a$ or $|v\rangle_a$ of the external photon in mode a is copied, after being flipped ($h \leftrightarrow v$), onto Alice's friend's photon in mode α. In other words, this corresponds to a measurement of the incoming photon in the $\{h, v\}$-basis, with the outcome being recorded in the state of photon α (Alice's friend memory), such that we can write

$$|\text{“photon is } h\text{”}\rangle_\alpha = |v\rangle_\alpha, \quad |\text{“photon is } v\text{”}\rangle_\alpha = |h\rangle_\alpha. \tag{4.30}$$

The amplitudes $\frac{1}{2}$ in Eq. (4.29) indicate the total success probability of $\frac{1}{4}$ for this procedure.

Bob's friend observation. This is equivalent to the Alice's friend observation with the relabelling $A \to B$, $a \to b$, $\alpha \to \beta$ and $\alpha' \to \beta'$.

Alice and Bob measurements. From Alice and Bob perspective, the overall quantum system is described by the state

$$|\tilde{\Psi}\rangle_{ab}|\Psi^-\rangle_{\alpha'\alpha}|\Psi^-\rangle_{\beta'\beta} \xrightarrow{FG_{\mathrm{I}}^{\otimes 2}} \frac{1}{4}|\tilde{\Psi}'\rangle_{a\alpha b\beta}, \tag{4.31}$$

with a global success probability of $\frac{1}{16}$. The state

$$|\tilde{\Psi}'\rangle_{a\alpha b\beta} = \frac{1}{\sqrt{2}}\cos\frac{\pi}{8}\left(|hv\rangle_{a\alpha}|vh\rangle_{b\beta} + |vh\rangle_{a\alpha}|hv\rangle_{b\beta}\right) + \frac{1}{\sqrt{2}}\sin\frac{\pi}{8}\left(|hv\rangle_{a\alpha}|hv\rangle_{b\beta} - |vh\rangle_{a\alpha}|vh\rangle_{b\beta}\right), \tag{4.32}$$

is the four-photon state shared by Alice and Bob when both fusion gates are successful.Note that, this state is a linear graph state. Recalling from Eq. (4.30) how the friends' measurement results are encoded in their polarisation states, the observables of Eq. (4.23) and Eq. 4.24 to be measured on $|\tilde{\Psi}'\rangle_{a\alpha b\beta}$ are

$$A_0 = B_0 = \mathbb{1} \otimes (|v\rangle\langle v| - |h\rangle\langle h|), \quad A_1 = B_1 = |\Psi^+\rangle\langle\Psi^+| - |\Psi^-\rangle\langle\Psi^-|, \tag{4.33}$$

More specifically, to measure A_0 (similarly B_0) we project onto $|hv\rangle_{a\alpha}$ and $|vv\rangle_{a\alpha}$ (eigenvalue $+1$), and $|hh\rangle_{a\alpha}$ and $|vh\rangle_{a\alpha}$ (eigenvalue -1). Note that A_0 cannot be simply measured by ignoring photon a, due to the probabilistic nature of the photon source. To measure A_1 (B_1) we project onto the singlet state $|\Psi^{\pm}\rangle_{a\alpha}$. The theoretically expected values for the various probabilities are either $\frac{1}{4}(1+\frac{1}{\sqrt{2}}) \simeq 0.427$, $\frac{1}{4}(1-\frac{1}{\sqrt{2}}) \simeq 0.073$, or 0.

4.4.5 Alternative Definition of A_0, B_0

Before moving to the experimental setup, we note that in Brukner's theory work [89] a different interpretation and definition for A_0 and B_0 are given. The author defines:

$$A_0' = B_0' = |h\rangle\langle h| \otimes |\text{“photon is } h\text{”}\rangle\langle\text{“photon is } h\text{”}| - |v\rangle\langle v| \otimes |\text{“photon is } v\text{”}\rangle\langle\text{“photon is } v\text{”}|, \tag{4.34}$$

which have a slightly different physical interpretation. The observables defined in Eq. (4.33) directly measure the facts established by the friend, as recorded in their memory. In contrast, the observables in Eq. (4.34) can be understood as not only a measurement of the friend's record (to establish a "fact for the friend"), but also of the original photon measured by the friend, as a consistency check: if the state of

the photon is found to be inconsistent with the friend's record, the definition above assigns a value 0 for the measurement result. Our experiment also allows us to test inequality (4.26) using this alternative definition of A'_0, B'_0. We assign in this case the eigenstate/eigenvalue according to $|hv\rangle \to +1$, $|vh\rangle \to -1$ and $|hh\rangle, |vv\rangle \to 0$ in the calculation of the average values $\langle A_x B_y \rangle$.

4.4.6 The Experimental Setup

With the help of Fig. 4.6, the experimental setup is described here in detail. This was aligned and characterised in approximately one month. The readers are referred to Chapter 3 for a detailed description of the working principles of each component.

A 775 nm, 1.6 ps-pulsed Ti:Sapphire laser is firstly filtered with a Faraday isolator and coupled into a hollow-core fibre to prevent beam misalignments in the setup. A hollow-core was chosen to avoid any non-linear effects due to the 2.4 W output power of the Ti:Sapphire.

At the fibre output, a 2.5 cm focal length lens collimates the beam with a FWHM of 2700 μm, which is then aligned to form a temporal multiplexing [92] scheme (also called interleaver). This increases the repetition rate of the pump laser from 80 MHz to 320 MHz, A.

The pump is focused with a 50 cm focal length lens into a 22 mm periodically-poled KTP crystal in a Sagnac-type interferometer [46], where it generates pairs of 1550 nm single photons through collinear type-II parametric down-conversion, B. We thereby achieve a signal-to-noise ratio (i.e. photon pairs vs. higher-order contributions) of 140 ± 10 in each photon source, generating $\sim$ 8000 photon pairs $\mathrm{mW}^{-1}\ \mathrm{s}^{-1}$ with a typical heralding efficiency $\eta = (cc/\sqrt{s_1 s_2})$ of $\sim$ 50%, where cc are the number of coincidence counts, and s_1, s_2 are the numbers of singles in the first and second output respectively. Single photons pass through 3 nm band-pass (BP) filters to guarantee high spectral purity. In the experiment, we use three of these sources: S_0, S_A and S_B. Effort was made to prepare all the three sources to be as similar in performance as possible. However, a typical systematic error on the brightness and heralding of 3% of the values reported above, was observed. This is mostly due to asymmetric coupling and slightly different beam waists for each path of the interleaver.

Each source is aligned to generate high-quality entangled states, see Sec 3.5. We consider the state generated at the output of the source to be:

$$|\Psi^-\rangle = \frac{|h\rangle|v\rangle - |v\rangle|h\rangle}{\sqrt{2}}, \tag{4.35}$$

which can then be mapped into any of the Bell states by means of local operations on one of the two qubits. We confirm the almost ideal quality of the prepared states via quantum state tomography. All the sources exhibited typical fidelities of $F = 99.62^{+0.01}_{-0.04}\%$, purity $\mathcal{P} = 99.34^{+0.01}_{-0.09}\%$ and entanglement as measured by the concurrence $\mathcal{C} = 99.38^{+0.02}_{-0.10}\%$, see Section 2.6 for definitions of these quantities.

All sources are connected trough fibres to their respective type-I fusion gate [47], a building block for any multi-photon experiment, C. After the transmission in fibre, the states fidelities were slightly degraded resulting in $F_0 = 98.79^{+0.03}_{-0.03}\%$, $F_A = 98.70^{+0.03}_{-0.03}\%$, $F_B = 98.59^{+0.03}_{-0.03}\%$ for sources S_0, S_A and S_B respectively. This unexpected effect might be due to imperfect identity operations from the fibre polarisation controllers.[5]

The expected behaviour of the fusion gates is verified by means of an Hong-Ou-Mandel experiment whose visibility, as given by the indistinguishability (in all degrees of freedom) of the interfering photons, represents an upper bound for the entangled state's polarisation purity. We achieve a typical visibility of $91.80 \pm +1.73\%$ with a pump power of 100 mW. This value is $\sim 4\%$ lower then what should be expected with our kind of apparatus and, although a very careful investigation was conducted, no evident causes of the degradation were found.[6]

Finally, photons are measured D. The setup is prepared to measure either

[5] In this regard, the standard procedure for the correct functionality of the polarisation controller, is to apply a specific number of loops inside each of their three pads. This is advised to be (2,3,2) loops for the first, second and third pad respectively. However, such configuration was measured to introduce from 1 % to 2 % of losses due to the tight bend radius of the fibre inside the pads. Therefore, the number of loops was decreased to (1,2,1) to eliminate losses. This expedient might have however limited the capability of each polarisation controller to perform any possible rotation in the polarisation space, explaining the slightly degraded fidelities. Purity and entanglement are instead preserved as few meters of fibre only introduce negligible non-unitary noise.

[6] Only very recently (more than one year after this work) the problem was actually found to be caused by the hollow-core fibre which we employed for the beam stability. Experimental evidence (observed for the first time by my colleague Alex almost by chance) showed that the interference visibility could be increased by decreasing the amount of power going through the hollow-core fibre (keeping fixed the power at the crystal). A sensible physical explanation to this phenomenon was not found, and never will be.

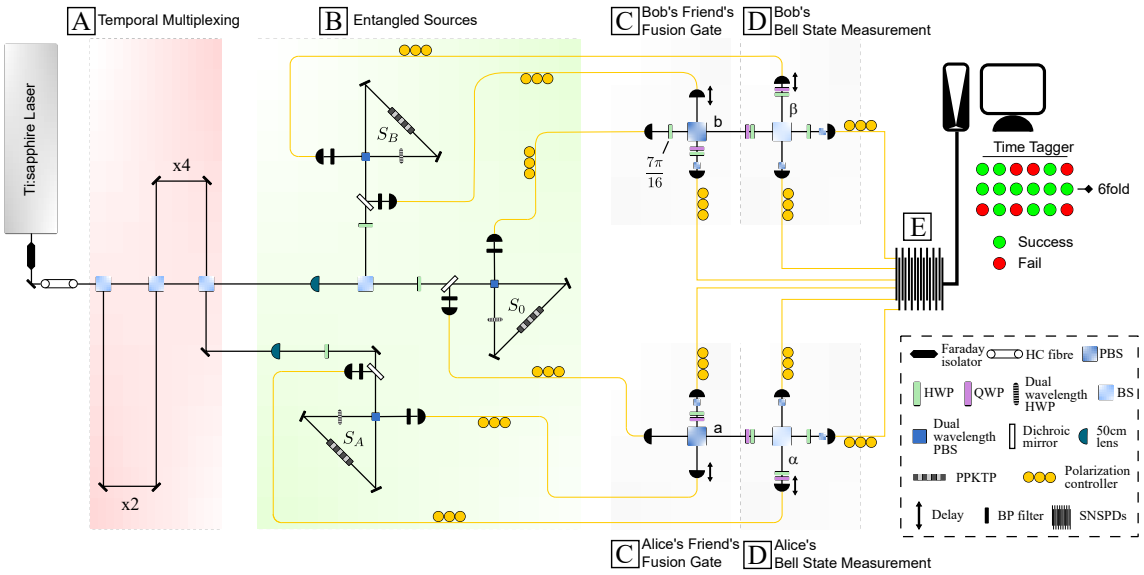


Figure 4.6: **Detailed experimental setup.** The Ti:Sapphire laser beam is protected from back-reflections by a Faraday isolator and spatially filtered using a short hollow-core fibre. The laser beam is then temporally multiplexed to effectively quadruple the pulse rate. The pump is then focussed to three Sagnac-interferometer sources to create polarisation entangled photon pairs. The outputs of each source are coupled to single-mode fibres and delivered to the measurement stages. Fibre polarisation controllers are used to maintain the polarisation states of the photons during transport. The three entangled pairs are then subject to two fusion gates, where temporal mode matching is achieved by employing physical delays as indicated. One photon at each measurement stage acts as a heralding signal for the success of the fusion gate, while the other two are subject to a Bell-state measurement on a 50/50 beam splitter, or to a direct measurement without the BS (for A_0, B_0), followed by projection onto orthogonal polarisations. Finally, all six photons are fibre-coupled and detected by the SNSPDs whose detection is processed by a classical computer to find 6-photon coincidence events.

the observables defined in Eq. (4.33). A_0, B_0 are a Z-base measurement realised with a polarisation beam splitter (PBS), where the transmitted and reflected ports correspond to the σ_z eigenvalues $+1$ and -1 respectively. This, however, would require two detectors per PBS, which was not possible in our case. The solution is simply to add a HWP before the PBS to switch between the h-projection and v-projection. The result is the same, but the time required for the data acquisition is doubled. A_1, B_1 require a projection in one of the Bell-states which can be done experimentally with 1/2 probability, by means of two-photon interference into a beam splitter (BS). Experimentally, we reproduce the expected projection with a fidelity of $F_{\text{BSM}} = 96.84^{+0.05}_{-0.05}$, as verified by quantum measurement tomography. Projections on the other Bell states are possible via local rotations using QWP and

HWP.

In principle, switching between the two types of measurement (A_0, B_0) and (A_1, B_1) would be required. In the experiment we use two different approaches: the first is to manually add two crossed polarisers before the BS when measuring (A_0, B_0); the second is instead to remove the BS whenever (A_0, B_0) are measured, and to place it back when (A_1, B_1) are measured. Although the former is the least invasive method as a polariser can be introduced in the setup without disruption, the latter can increase the probability of success of the (A_0, B_0) measurements. In fact, the polariser effectively measures the photons in modes a (b) and α (β) before the BS, preventing interference. However, as the BS does not distinguish between $|h\rangle$ and $|v\rangle$, the expected eigenstate is measured only with probability 1/4. For example, if we want to measure the eigenstate $|hv\rangle_{a\alpha}$ we want the photons to be reflected and transmitted respectively, which happens with 1/4 probability. Conversely, by removing the BS and without adding polarisers, the probability of successfully measuring (A_0, B_0) is 1. Overall, with this strategy, we increase the probability of measuring A_0B_0, A_1B_0 and A_0B_1 by a factor 16, 4 and 4 respectively.

We note that removing the BS and placing it back does not perfectly recover the beam alignment. To limit this effect, we use magnetic bases for the BS prism table, such that the alignment could be recovered quite easily. But what is mainly effected by the removal operation is definitely the quality of the two-photon interference necessary for the Bell-projection. Varying the position of the BS by few microns, can decrease the interference visibility and therefore the BSM fidelity. Fortunately, recovering the maximum visibility only takes few minutes in our setup. In fact, we can monitor the two-photon interference of the photons arriving at the BS from the same source. This approach enabled the collection of all required data with good statistics in a reasonable amount of time. Nevertheless, a set of data with the linear polarisers in place instead of the BS removal procedure was taken, and used to show an alternative violation of the Bell-Wigner inequality using Brukner's definition of the observables in Eq. (4.34).

The experiment ends with the photon detection $\boxed{\text{E}}$. Photons are detected with superconducting nano-wire single-photon detectors (SNSPDs) with a detection efficiency of $\sim$80% and measured dark counts of $\sim$100 Hz. Detector clicks are time-

tagged using a field-programmable gate-array (FPGA) and processed to detect coincidences within a temporal window of 1 ns. We postselect only on the events where six photon coincidences are realised, which can happen only when all the three sources generate at least one pair of photons.

We observe, at 100 mW and using the BS removal procedure, a six-fold coincidence rate of 0.053 Hz, 0.022 Hz, 0.021 Hz and 0.015 Hz for A_0B_0, A_0B_1, A_1B_0 and A_1B_1 respectively. We observe, at 100 mW and without the BS removal procedure, a six-fold coincidence rate of 0.0031 Hz, 0.0071 Hz, 0.0067 Hz and 0.015 Hz for A_0B_0, A_0B_1, A_1B_0 and A_1B_1 respectively. As noted above, if the BS is removed when either A_0 or B_0 are measured, the raw experimental generation rates are ~ 16 times and ~ 4 times higher for A_0B_0 and A_0B_1/A_1B_0 respectively. These rates could be increased by increasing the pump power. However as outlined in Sec 3.1 with the signal-to-noise ratio dependence on pump power, increasing the pump power degrades the quality of the single-photon sources. The power used in the experiment was set on the base of previous tests, suggesting 100 mW to give an acceptable trade off between the quality of the sources and the 6-fold rates.

4.4.7 Results

We estimate the four average values $\langle A_x B_y \rangle$ in inequality (4.26) via projection onto each of the 4×4 eigenstates of the observables A_x and B_y. For $\langle A_0B_0 \rangle$, we collect 479 six-fold events in 2.5 hours per eigenstate, obtaining an expectation value of $-0.678^{0.033}_{0.033}$. For $\langle A_0B_1 \rangle$, we collect 405 six-fold events in 5 hours per eigenstate, obtaining an expectation value of $0.570^{0.040}_{0.040}$. For $\langle A_1B_0 \rangle$, we collect 378 six-fold events in 5 hours per eigenstate, obtaining an expectation value of $0.595^{0.041}_{0.041}$. Finally, for $\langle A_1B_1 \rangle$, we collect 532 six-fold events in 10 hours per eigenstate, obtaining an expectation value of $0.571^{0.034}_{0.034}$. In total, for the full 64 settings, we measured for 360 hours collecting 1794 six-photon coincidence events, from which we calculate the probabilities shown in Fig. 4.7. With these data, we achieve a value of $S_{\text{exp}} = 2.416^{+0.075}_{-0.075}$, thus violating inequality (4.26) by more than 5 standard deviations.

We repeat the experiment, with two polarisers before the BS and applied the alternative definitions A'_0 or B'_0 given in Eq (4.34). In this case, due to the drastic decrease of the success probability, we do not measure all the 64 eigenstates, but for

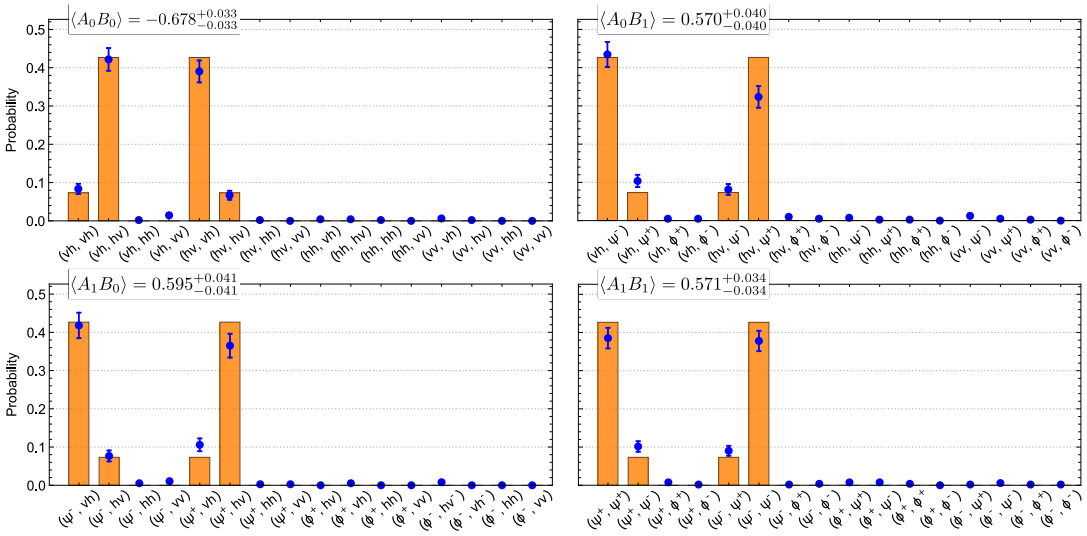


Figure 4.7: **Full experimental data for the 64 settings**. The horizontal axis in each of the four plots indicates the eigenstates (φ_A, φ_B) on which the experimental state shared by Alice and Bob in Eq. (4.32) is projected, where φ_A corresponds to Alice's projection in the two modes a and α, φ_B instead represents Bob's projection in modes b and β. For each setting, the number of 6-photon coincidences is recorded and normalised to obtain the relative probabilities as shown in the vertical axis.

the observables $A'_0B'_0$, $A_1B'_0$ and A'_0B_1 we collect six-fold events only for the four non-zero eigenstates and compute the expectation values with the normalisation given by the 16 settings of A_1B_1. For $\langle A'_0B'_0\rangle$, we collect 446 six-fold events in 40 hours per eigenstate, obtaining an expectation value of $-0.609^{0.048}_{0.048}$. For $\langle A'_0B_1\rangle$, we collect 509 six-fold events in 20 hours per eigenstate, obtaining an expectation value of $0.577^{0.049}_{0.049}$. For $\langle A_1B'_0\rangle$, we collect 485 six-fold events in 20 hours per eigenstate, obtaining an expectation value of $0.588^{0.049}_{0.049}$. In this experimental run, we measured for 320 hours collecting 1440 six-photon coincidence events, from which we calculate the probabilities shown in Fig. 4.8. With these data, we achieve a value of $S_{\text{exp}} = 2.346^{+0.110}_{-0.110}$, thus violating inequality (4.26) by more than 3 standard deviations. We note that the violation observed with this method is somewhat reduced because of $\sim 4.83^{0.97}_{0.97}\%$ loss that is introduced by the polarisers. This effectively reduces the number of counts that are observed in the settings A'_0 and B'_0 compared to the normalisation used, and thereby reduces the expectation values $\langle A'_0B_1\rangle$ and $\langle A_1B'_0\rangle$, and $\langle A'_0B'_0\rangle$, leading to a reduced violation.

Overall, the complete data collection was obtained in 680 hours, taken in the period from the 10th of May to the 8th of July, 2018.

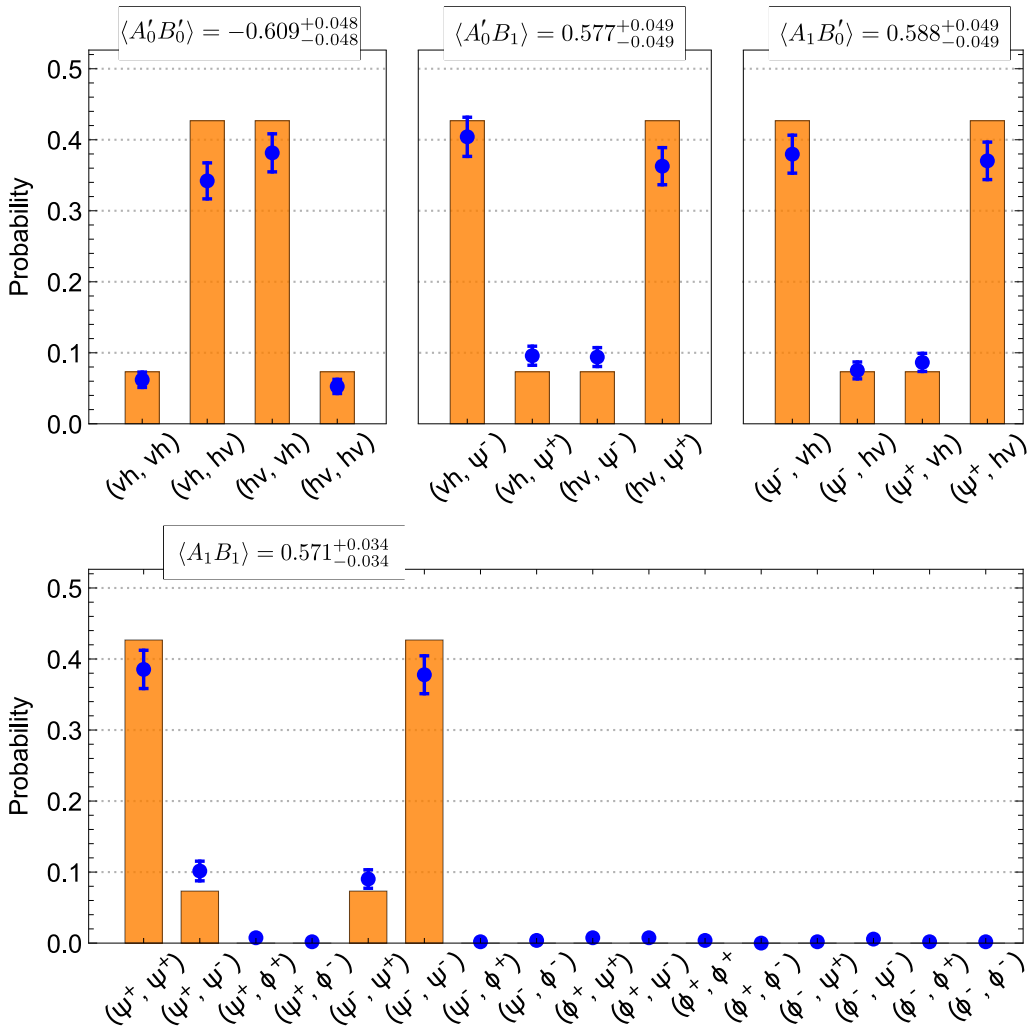


Figure 4.8: **Alternative protocol experimental data**. The experimental probabilities obtained with the alternative definition of A_0 and B_0, Eq. (4.34), are shown. $\langle A_1 B_1 \rangle$, in the bottom panel, is left unchanged by the new definition thus the data shown here as well as the average value for this couple of observables, is the same as in Fig 4.7. Moreover, $\langle A_0' B_0' \rangle$, $\langle A_0' B_1 \rangle$ and $\langle A_1 B_0' \rangle$ shown in the top panels are measured adding the crossed polarisers before the BS as explained in Sec 4.4.6 . In this case, only 6-photon coincidences for the non-zero terms, labelled in the horizontal axis, are recorded and normalised with the sum of all the coincidences recorded for $\langle A_1 B_1 \rangle$.

4.4.8 Error Analysis

Each average value $\langle A_x B_y \rangle$ reported previously is calculated from 16 measured 6-fold coincidence counts n_i. These numbers follow a Poisson distribution with variance $\sigma^2_{n_i} = n_i$. The uncertainty on $\langle A_x B_y \rangle = f(n_1, \ldots, n_{16})$ can then be computed using

$$\sigma_f^2(n_1, \ldots, n_{16}) = \sum_{i=1}^{16} \left(\frac{\partial f}{\partial n_i} \right)^2 \sigma^2_{n_i}. \tag{4.36}$$

Since the four averages $\langle A_1 B_1 \rangle$, $\langle A_1 B_0 \rangle$, $\langle A_0 B_1 \rangle$ and $\langle A_0 B_0 \rangle$ are statistically independent, the uncertainties can be calculated independently and combined to estimate the uncertainty on S. To take into account potentially asymmetric errors in the limit of small count rates, we computed the uncertainty on the Bell-Wigner parameter S using a Monte-Carlo routine with 100000 samples. The difference between the values obtained through these two methods is negligible.

Note that in the results shown in Fig. 4.8 with the observables of Eq.(4.34), errors are correlated due to normalisation with a common total. Accounting for this in the error propagation results in slightly larger statistical uncertainty.

The Bell-Wigner value S_{exp} that can be achieved experimentally is limited by multi-pair emissions from our probabilistic photon-pair sources. We first note that any emission of three pairs from any subset of our three sources occurs with roughly similar probability. To exclude unwanted terms we use six-fold coincidence detection, which can only be successful for an emission of one pair each in S_0, S_A and S_B, or three pairs in S_0. The latter would amount to noise but is excluded by our cross-polarisation design and can thus not lead to a coincidence detection. This leaves higher-order contributions where at least 4-photon pairs are produced as the main source of errors. Since such events scale with a higher exponent of the pump power, they are suppressed in our experiment by working with a relatively low pump power of 100 mW.

Moreover, the limited visibility of the interference at the fusion gates, sets an upper bound to the maximum experimental value of S_{exp}, as unsuccessful fusion effects the coherence of the output pairs without effecting their polarisation, leading to lower values of A_1 and B_1. This systematic error is hard to prevent, as it is intrinsic of the photons' spectral properties, which can only be modified by hard spectral filtering (lowering however the effective counts) or by engineering the PDC crystals [93].

4.5 Discussion

With the observed violation of inequality (4.26), we demonstrated that our data can not be explained by any theory where the assumptions of locality, freedom of

choice and observer-independence concurrently hold true. This statement however, is sustained by the observer definition we provided, enabling single photons to play this role. If the definition is disputed, so will our conclusions. However a convincing revision of our minimal definition of what qualifies as an observer, would require new physics that is not described by standard quantum theory. Eugene Wigner, for example, argued that the disagreement with his hypothetical friend could not arise due to a supposed impossibility for conscious observers to be in a superposition state [67]. However, the incompatibility between locality, freedom of choice and observer independence does not arise in anyone's consciousness, but between the recorded facts. Since quantum theory does not distinguish between information recorded in a microscopic system (such as our photonic memory) and in a macroscopic system, the conclusions are the same for both: the measurement records are in conflict regardless of the size or complexity of the observer that records them. Implementing the experiment with more complex observers would not necessarily lead to new insights, beside showing that quantum mechanics still holds at larger scales, ruling out alternative (collapse) models [65]. However, this is not the point of a Bell-Wigner test—less demanding tests could show that. On this regard the reader is pointed to Ref. [94] for a result claiming that the existence of a macro-scale beyond which the quantum formalism becomes superfluous is unjustifiable from an information-theoretic perspective. The theory as in Ref. [94] was experimentally tested by our group and the results are given in Appendix B.

It should be noted that the results of our Bell-Wigner test directly derive from Brukner's theory [89] and the assumptions therein. In particular as noted in [95] Brukner's claim relies on an additional assumption which has not been mentioned so far. This states that there exists a truth value about the results of all measurements, even ones Wigner chose not to perform, which is equivalent to assuming all possible measurement outcomes being predetermined by hidden variables. Brukner postulates this to be true. According to Ref. [96], this is a very strong assumption which could impact the validity of Brukner's theorem itself. However it was shown in the same Ref. [96] that the theorem can be proven without the need of such postulate. Moreover, it was formally shown that any Bell-Wigner violation implies a Bell-violation, but not the other way round.

Finally, we discuss our result in comparison with a related but independent work from Frauchinger and Renner (FR) [97]. In their work, the authors employ an extended Wigner's friend scenario to show that quantum mechanics predictions are incompatible with the joint assumptions of the universal validity of quantum theory (Q), consistency of the theory (C) and single-outcome measurements (S). Importantly, FR result involves agents rather than observers (see Sec 4.4.6). The assumption Q more precisely states that an agent can be certain that a given proposition holds whenever the quantum-mechanical Born rule assigns probability-1 to it. Assumption C states that different agents' predictions are not logically contradictory. Assumption S states instead that from the viewpoint of an agent who carries out a particular measurement, this measurement has one single outcome. Quantum mechanics is not compatible with all the three assumptions, and at least one of them must be violated, according to FR. Clearly, single photons can not be valid agents and therefore our setup can not be employed to demonstrate FR result and we leave as an open question whether agents can be realised experimentally in a controlled way.

4.5.1 Detection and Locality Loophole

In principle, "Bell-Wigner tests" like ours are subject to similar loopholes as tests of conventional Bell inequalities [98] (see Sec 4.3 for a review of the loopholes). However, due to the increased complexity of our experiment, compared to a standard Bell test, the practical requirements for closing these loopholes are significantly more challenging. The configuration of our experiment could be analogous to an "event-ready" Bell test [99], where the detection of the ancilla photons in the fusion gates heralds which events should be kept for the Bell-Wigner test. Nevertheless, to ensure that the fusion gates are indeed event-ready, the ancilla detectors should be photon-number-resolving, which is not the case in our experiment. Moreover, to measure the observables A_x, B_y, we chose to project the photon states onto their different eigenstates separately. To close the detection loophole one cannot follow such an approach: the measurement protocol should be able to project the states onto all of the eigenstates in any run of the experiment. To measure A_0/B_0 from Eq. (4.23), one could pass the friend's photon through a PBS, with detectors at both outputs.

As for A_1/B_1, a complete Bell-state measurement (which is impossible with linear quantum optics [100]) is not required: it suffices to distinguish $|\Psi^+\rangle, |\Psi^-\rangle$, and have a third outcome for $|\Phi^\pm\rangle$ (see Eq. (4.33)). This can be realised with a small modification to our setup, with detectors added on the second outputs of Alice's and Bob's PBS [101]. An even simpler measurement would discriminate e.g. $|\Psi^-\rangle$ from the other three Bell states, thus measuring the observables $A_1 = B_1 = \mathbb{1} - 2|\Psi^-\rangle\langle\Psi^-|$ with outcome -1 assigned to $|\Psi^-\rangle$ and outcome $+1$ to all the other Bell states; this would not change anything in an ideal implementation, but simplifies the analysis with detection inefficiencies below.

We assume a symmetric combined detection efficiency per photon of η i.e. the probability $P(A|B)$ that detector A clicks given that detector B has clicked. The measurement of A_0/B_0 requires one detector to click and would succeed with probability η, in particular we have $P(d_a|d_b) = P(d_b|d_a) = \eta$ where d_a and d_b are the detectors in modes a and b respectively, see Fig. 4.5. The measurement of A_1/B_1 requires instead two detectors to fire and would work as expected with probability η^2. When a detector fails to click, a simple strategy is to output a fixed pre-defined value for the measurement outcome, e.g. $+1$. Then, the average values $\langle A_x B_y\rangle$ are theoretically expected to be $\langle A_0 B_0\rangle = \eta^2(-\frac{1}{\sqrt{2}}) + (1-\eta)^2$, $\langle A_0 B_1\rangle = \langle A_1 B_0\rangle = \eta^3 \frac{1}{\sqrt{2}} + (1-\eta)(1-\eta^2)$ and $\langle A_1 B_1\rangle = \eta^4 \frac{1}{\sqrt{2}} + (1-\eta^2)^2$. With these values, the minimal required detection efficiency to violate inequality (4.26) with (unrealistically) perfect quantum states and measurements is $\eta > 2\sqrt{3(1-\frac{1}{\sqrt{2}})} - 1 \simeq 0.875$. Experimentally closing the detection loophole with a photonic setup might be challenging. In fact, assuming only single-pair generations from the three sources, we have that every time both the fusion gates click there must be four photons in the spatial modes a, b, α and β, see Fig. 4.5. We consider the geometric mean of the symmetric detection efficiencies given by $\sqrt{P(d_a|d_b)P(d_b|d_a)} = \eta$ and we note that $\sqrt{P(d_a|d_b)P(d_b|d_a)} = P(d_a, d_b)/\sqrt{P(d_a)P(d_b)}$ where $P(d_a, d_b)$ represents the probability that both d_a and d_b fire whereas $P(d_a)$ ($P(d_b)$) is the probability that only detector d_a (d_b) fires. Experimentally, we can obtain $P(d_a, d_b)$ from the coincidence events of detectors d_a, d_b and $P(d_a)$ ($P(d_b)$) from the singles. Note however that once we take into account the two heralding detections at the fusion gate $P(d_a, d_b)$ describes a 4-photon coincidence event whereas $P(d_a)$ ($P(d_b)$) represents a 3-photon

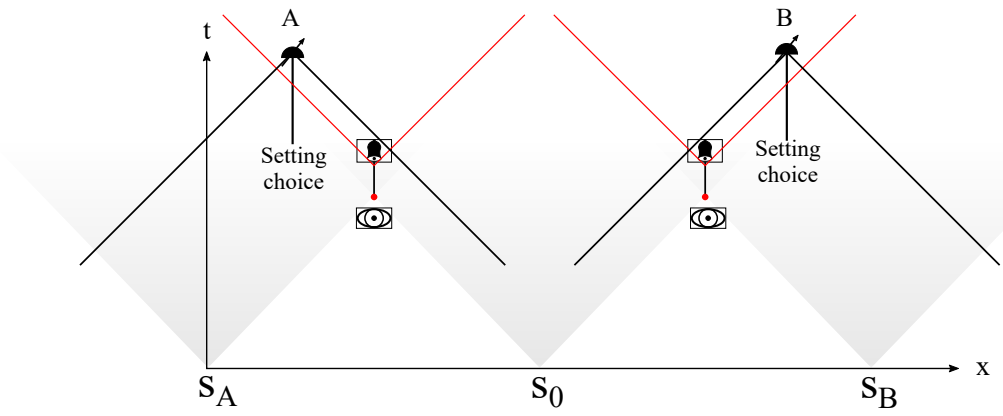


Figure 4.9: **Space-time diagram of the Bell-Wigner test.** The three single photon sources S_A, S_0 and S_B generate at the same time but at different locations the pairs of entangled photons. The friends measurements are labelled with an eye in the figure, and the two heralding events happening in the same location but a later time are shown with a bell symbol. Importantly, the setting choice events must be outside the light cone of the two heralding events, as shown in the figure. Finally, after the setting choice the Alice and Bob detections take place and have to be independent from the setting of the other party.

coincidence event. With our sources, the value of η in the experimental implementation reported in this chapter was on the order of 10^{-2} therefore far from the target threshold of 0.875. More on alternative ways of closing the detection loophole in a Bell-Wigner test are discussed in the conclusions section, Sec. 4.6.

The locality loophole instead requires the heralding events to be space-like separated from Alice's and Bob's setting choices, which should each be space-like separated from the measurement outcome of the other party. This imposes stringent space-time location requirements for a Bell-Wigner test closing these loopholes, see Fig. 4.9. In particular, this demands the capability of delivering multi-partite entangled states for long distances, a notable challenge with current technologies.

Note, finally, that in the conclusions we draw from the violation of inequality (4.26), we need to trust that A_0 and B_0 indeed directly measure the memory of Alice's and Bob's friends, so as to unveil their respective facts. A new loophole may be opened, now specific to Bell-Wigner tests, if such an interpretation cannot be maintained. To address this loophole with a setup like ours, one should use measurement devices for A_0 and B_0 that clearly separate the initial systems and the memories of each friend, and only "looks" at the memory photons, rather than at the system photon + memory photon together; we also leave this possibility as a

challenge for future Bell-Wigner experimental tests.

4.6 Conclusions

In this chapter we showed modulo the potential loopholes and accepting the photons' status as observers, the violation of inequality (4.26) implies that at least one of the three assumptions of freedom of choice, locality, and observer-independent facts must fail.

Refuting the freedom of choice assumption would imply that the hidden variables and the settings are not independent. If we assume λ to be created with the photons at the sources, refuting F would open as a possibility retro-causal signals [102] from the setting choice event back in time to the λ creation. This approach is the preferred by the supporters of the transactional interpretation of quantum mechanics, based on a retro-causal model [103]. Another option is to assume that the choice of the setting is not free but causally influenced by other variables, also known as superdeterminism.

Giving up the locality L assumption instead would imply faster-than-light signals propagating from Alice's setting choice event to Bob's measurement and vice versa[7]. This would be in contrast with Einstein's relativity. Non-local theories giving the same predictions of quantum mechanics such as Bohmian mechanics [60] embrace this option (see Sec. 4.1).

One more way to accommodate our result is by proclaiming that "facts of the world" can only be established relative to an observer as in the relational quantum mechanics [104], or by adopting an interpretation such as QBism, where quantum mechanics is just a a tool that captures an agent's subjective prediction of future measurement outcomes [105]. We note that also in Einstein's relativity there is a notion of relativism with respect to observers. However, conversely from Einstein's theory where different observers can ultimately reconcile their descriptions of a physical system, in our scenario refuting observer independence requires us to embrace the possibility that different observers irreconcilably disagree about what happened

[7]Note however that without access to the values of λ, in accordance with Einstein's theory, no information can be sent with a faster-than-light signal as the measurement outcomes will appear as a random string with no information.

in an experiment.

Which of the three assumptions between F, L, and O should be set as false, is left to the readers who accept our photons as valid observers. The author of this thesis does not have a firm position in this regard, however the rejection of observer independence could be the preferred option. Not only unperformed measurements have no results [106], but once they have, the result is a "fact of the world" [89] only relative to the observer who established it.

Future directions for research will be to address the two main loopholes as discussed in Sec 4.5.1. In particular, PDC sources seem to not be a valid candidate for this task. Inspired by recent advances towards atom-atom long distance entanglement [107] and based on a previous loophole-free Bell test with the same platform [108], using atoms for a loophole-free Bell-Wigner test might be a valid possibility. Similarly, entanglement between nitrogen-vacancy (NV) electron spin qubits and telecom-band photonic qubits was recently observed. [109]. Moreover multi-qubit entanglement between one electron spin and nine surrounding nuclear spins was recently observed [110] posing this type of platform as a valid candidate for a loophole-free Bell-Wigner test. Testing the Bell-Wigner inequality with one of these quantum technologies might however present new challenges, in fact high-quality multi-qubit entanglement is required. But more importantly, in our test with photonic qubits the experimental realisation of the Wigner's friend observation was achieved by means of the fusion gate. Therefore some equivalent mechanism is required in other platforms.

Furthermore, the violation of Bell inequalities witnesses the impossibility of some causal models to explain quantum correlations [111–113]. Similarly, the violation of Bell-Wigner inequalities can unveil new causal structures failing to reproduce the observed quantum correlations in a Bell-Wigner scenario.

Finally, going beyond the foundations of quantum mechanics, the Bell's theorem is now often invoked in the field of quantum key distribution whereby a secret key has to be shared in a device-independent way [114]. We might then expect our Bell-Wigner inequality to be used as a resource for some more technical result of quantum information.

Chapter 5

Experimental Conference Key Agreement

In this Chapter I present the first experimental realisation of a conference key agreement (CKA) protocol. CKA protocols enable several users to establish a common and secret key to be consumed for example to encrypt a conference call. The security of the conference key is guaranteed by the laws of quantum mechanics. The experiment I show in this chapter is envisioned to pave the way for a new class of quantum protocols to be embedded with the flourishing quantum network technologies.

I will start in Sec. 5.1 with a brief review of the well-known field of quantum key distribution (QKD). I follow in Sec. 5.2 with the so-called error correction and privacy amplification, two classical routines required to the establishment of a secret key. I then move from the canonical 2-party scenario to the multipartite case, introducing a conference key agreement protocol in Sec. 5.3. I present the experimental realisation of the CKA protocol in Sec. 5.4 and in Sec. 5.5 the experimental results are presented. Furthermore, in Sec. 5.6 I describe a new problem arising in conference key agreement which is the dependence of the key rates on the network topology. Finally, discussion and conclusions are outlined in Sec. 5.7.

I note that some of the text in this chapter is excerpted from the research paper in Ref. [115], where I led the experimental development of the project, from the characterisation and preparation of the full experimental setup to the data acquisition and data analysis.

5.1 Quantum Key Distribution

In 1917 Gilbert Vernam invented the so called one-time pad encryption protocol [116], which was proved in 1949 by Claude E. Shannon to be "information-theoretically secure" i.e. its security is independent from the adversary computing power [117]. The protocol requires two users to share a random secret key consumed only once to encrypt and decrypt a message and it was proven by Shannon to be optimal in the sense that the encryption process does not reveal any additional information about the message to be encrypted. Thus, the security of the key consumed for the encryption is paramount. Quantum key distribution can provide the sender and receiver with a common information-theoretic secret key, therefore embedding QKD with the one-time pad encryption provides a method for sharing unconditionally secure messages, the holy grail of cryptography. As we will see in the following, the key feature about QKD is that the laws of quantum mechanics permit to estimate how much information was leaked during the exchange of the key, hence allowing the users to remove in post-processing that same amount of information from the shared key or even to abort the protocol when the security is irremediably compromised. The same is not possible in classical communication where information on the key can be extracted by an adversary without leaving any trace.

Building upon previous original ideas from Stephen Wiesner for the realisation of quantum banknotes [118] the term "Quantum Cryptography" was firstly coined in Ref. [119] where the Wiesner's scheme was merged with classical public-key cryptography principles. Shortly after these preliminary results, the first QKD paper was published in 1984 by Bennett and Brassard who proposed the now famous BB84 protocol [120]. Some years later a new quantum protocol for key distribution was introduced by Ekert [121], and the topic of QKD started to draw the attention of both the computer science and physics community.

In both protocols a quantum and a classical channel is employed, the former serves the transmission of the qubits encoding the key itself and can be manipulated by an eavesdropper with no restrictions. The latter is used to communicate classical messages needed to estimate the amount of information leaked during the key distribution and correct the key if errors occur. Importantly, the classical channel must

be authenticated [122] i.e. an eavesdropper can listen to the conversation but can not impersonate either Alice or Bob. This is a requirement to avoid the so-called man-in-the-middle attack. The authentication requires a preshared secret key, hence quantum key distribution shall be seen as a key growing algorithm: secrecy can only grow but not be created. If these conditions are met, QKD can provide unconditional security. However, it is important to note, that in practice implementing a theoretical protocol with the available experimental resources presents several problems. For example, one common approach to experimentally implement a QKD protocol is by using weak coherent-states to send and distribute the key. However, it was then realised that as a weak coherent-state can sometimes contain more than one single photon, the security of the key could be compromised. In fact, in 1995 the so-called photon-number splitting (PNS) attack [123, 124] was proposed and shown to compromise the security of certain QKD protocols such as the BB84. In fact, if in one round more than one photon is employed to encode the same single qubit, the no-cloning theorem does no longer hold as multiple copies of the state are available and information leakage can not be estimated correctly by Alice and Bob. Nevertheless, the security of the protocol was recovered at the cost of lower key rates with the help of the decoy-states protocol [125–128], developed in 2003 for these purposes. This is a nice example of how theory and experiment have chased each other over time leading to modern QKD, a well-established quantum technology.

5.1.1 BB84

Consider the scenario depicted in Fig. 5.1 a. Alice (the sender) holds a single-photon source which she can control to prepare photons in either the Z-basis: $\{|h\rangle, |v\rangle\}$ or in the X-basis: $\{|d\rangle, |a\rangle\}$. The bit 0 is encoded with either $|h\rangle$ or $|d\rangle$, whereas the bit 1 is encoded with either $|v\rangle$ or $|a\rangle$. Alice randomly picks a basis and a state which is then sent to Bob (the receiver) through the quantum channel. In turn Bob will randomly select a basis and perform a quantum measurement, whose outcome is stored in some memory. The procedure is repeated L times and eventually Bob will obtain a string of L bits randomly distributed, this concludes the quantum part. The next steps are fully classical and operated by communication over the authenticated classical channel. Ideally, if the quantum channel preserved the state of the photons

at every round, Alice and Bob will hold the same bit when the preparation basis and measurement basis were the same, that is half of the rounds on average. Thus, in order to discard all the mismatched bits, Alice announces for each round the preparation base and Bob the measurement basis so that the two parties discard all the bits where they measured in a different basis. What is left is the raw key, identical in the ideal case. In general however, Bob's key will present errors due to either noise in the channel or an external intervention of Eve (the eavesdropper). In order to ensure security, all the errors are assumed to be due to Eve. Quantum mechanics enables the estimation of the information leaked during the transmission of the single photons, by measuring the quantum bit error rate (QBER). Alice and Bob agree on broadcasting a subset of the raw key and count the percentage of errors in that subset i.e. the frequency of a bit-mismatch event, namely the QBER. If the QBER is higher than some threshold they abort, otherwise they proceed to correct the raw key with some classical algorithm at the cost of revealing part of it. Finally, the now corrected key is made secret in privacy amplification (PA) by reducing its length according to the amount of information revealed during EC. In particular, this can be done using a universal hash function, chosen at random from a publicly known set of such functions, which takes as its input the corrected key and outputs a binary string (the secret key) of a chosen shorter length.

The security of the BB84 protocol against the most general coherent attacks (see [129] for a catalogue of the possible attacks in QKD) was demonstrated in 2000 by Shor and Preskill [130] by noting how QKD protocols are strictly related to entanglement distillation [6] and error correction theory. The rate of secret bits per round in the limit of $L \to \infty$ is given by the very simple and elegant expression

$$r_{\mathrm{BB84}} = 1 - h(e_z) - h(e_x), \tag{5.1}$$

where $h(x)$ is the Shannon binary entropy [131] and e_z, e_x errors in the Z-basis and X-basis respectively. When $e_z = e_x = e$ the threshold for a non-zero key is $e \approx 11\%$. BB84 is just one instance of a family of protocols called prepare-and-measure always involving a sender preparing single qubits then measured by the receiver. Other examples are the 6-state protocol [132] and the B92 protocol [133] which can show different noise tolerances and rates when compared to the BB84.

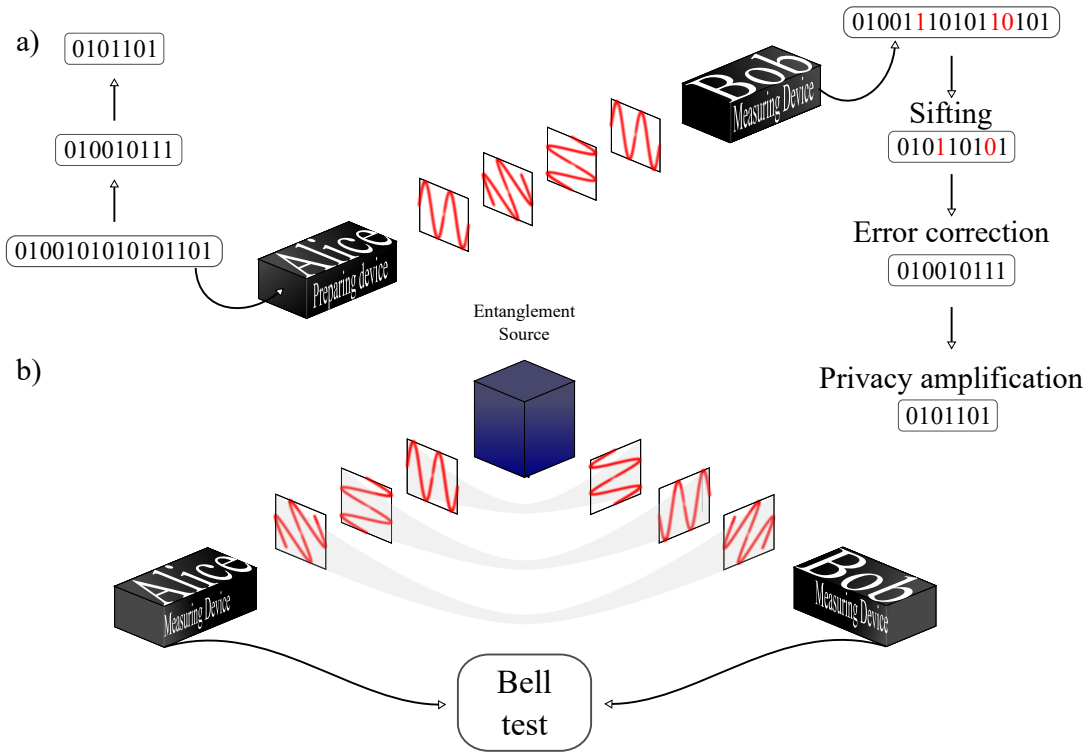


Figure 5.1: **a) BB84 protocol.** Shown is the concept of a prepare-and-measure QKD protocol such as the BB84. Only the rounds where the preparation and measurement base matches are kept (sifting), hence reducing the string size by half in average and leading to the raw key. This might contain errors, which are classically corrected at the cost of reducing the key size during privacy amplification. **b) E91 protocol.** As for entanglement-based protocols, a server prepares entangled photon-pairs which are measured in different bases. The classical post-selection routine is the same as in the BB84 with the addition of a Bell-test performed to enhance the key security.

5.1.2 E91 Protocol

The protocol introduced by Ekert in 1991 is the first example of an entanglement-based QKD protocol. Instead of relying on the impossibility of perfectly copying single qubits [134], it exploits the quantum correlations of maximally entangled states and the Bell theorem.

The protocol works as follows (see Fig. 5.1 b.), a source generates two single photons in one of the four Bell's states e.g. $|\psi^-\rangle$, then the two photons are sent to Alice and Bob respectively. Alice randomly measures in one of the three bases $\{X, \frac{X+Z}{\sqrt{2}}, Z\}$ whereas Bob measures randomly in one of the three bases $\{X, \frac{X+Z}{\sqrt{2}}, \frac{X-Z}{\sqrt{2}}\}$. The peculiarity of the singlet state $|\psi^-\rangle$ is that if Alice and Bob share the same polarisation reference frame, they will observe anticorrelated outcomes every time they

measure in the same basis. When instead they measure in a different basis they will compute a CHSH [74] (see Chapter 4, Sec. 4.3) inequality. Upon maximal violation of the inequality they are confident (within the laws of quantum mechanics) that their data is completely decoupled from any eavesdropper, and they keep all the bits derived from a same-basis measurement. In fact, recalling the meaning of the Bell's theorem [69], Eve's intervention can be seen as inducing elements of physical reality which affects the non-locality of quantum mechanics. In the QKD context it implies that upon violation of the inequality Alice and Bob can rule out the possibility of Eve controlling the source and their measurement device. This is also known as device-independent (DI) QKD and allows Alice and Bob to trust their keys, even if obtained by measuring qubits received from an untrusted source and measured with untrusted devices. The same result is not possible in BB84 using single qubits even in a noise-free scenario [135]. In practice however, the inequality will not be maximally violated and some amount of raw bits should be removed to account any possible information held by Eve. In particular, the secret key rate as a function of the CHSH value in presence of collective attacks was found in Ref. [136].

Following the idea introduced by Ekert, more entanglement-based protocols were proposed as for example the BBM92 [137], working more efficiently by having both the legitimate parties each measure in only two different bases instead of the three bases of E91.

5.2 Error Correction and Privacy Amplification

As noted in the previous sections, in any practical implementation of a QKD protocol, due to errors Bob's raw key will present some bit mismatch with respect to Alice's key. In order to correct those errors they resort to error correction which provides a solution to the problem. In general, some information will be disclosed during this process and can be used by Eve to obtain part of the key. If the amount of errors in the key is quantified by the QBER, the amount of information to disclose is lower-bounded by $h(\text{QBER})$, also known as the Shannon limit. Error correction codes can approach this limit for $L \to \infty$ and in practice the amount of information disclosed will be $f(\text{QBER})h(\text{QBER})$ where $f(\text{QBER}) > 1$ is some function of the

QBER and known as the code efficiency. Note that for an ideal (unrealistic) EC code $f(\text{QBER})h(\text{QBER}) = 1$.

Two different approaches are known: one-way and two-way error correction. The former requires Alice to send only once, enough information to Bob in order to correct his raw key. The latter requires Alice and Bob to iteratively communicate between each other until the keys are identical.

Following EC, Eve will retain partial information on the raw key and no security is guaranteed yet. Privacy amplification (PA) is invoked at this point in order to produce a new, shorter key, in such a way that Eve has only negligible information about the new key. In essence, this is achieved by randomly choosing a universal hash function, which takes as its input the raw key and outputs a new shorter key whose length depends on the estimation of the Eve's information of the raw key. This process reduces the probability of Eve having any knowledge of the new key to below some negligibly small, appropriately chosen threshold value.

In the following we review two EC protocols, the Cascade protocol and low-density parity-check codes.

5.2.1 Cascade Protocol

Suppose Alice and Bob hold some bit string S_A and S_B respectively. The task is to apply some operations on S_B in order to have $S_A = S_B$, by only means of two-way classical communication. The Cascade protocol [138] provides a routine to achieve this goal and it works as follow:

1. Alice and Bob randomly permute their keys obtaining new strings S'_A and S'_B respectively.
2. Alice and Bob divide their strings in partitions of k bits.
3. For each block b_j Alice and Bob compute the parity p_j.
4. Alice sends the parity bits to Bob who compares them with his parity bits for each block. If the parity bits are the same for all the blocks, Bob's key either do not contain any error or it contains an even number of errors. If for some block b_j the parity is different then an error is present in that block and they proceed to the next step.
5. The block b_j containing an error is split in half and Alice and Bob perform a

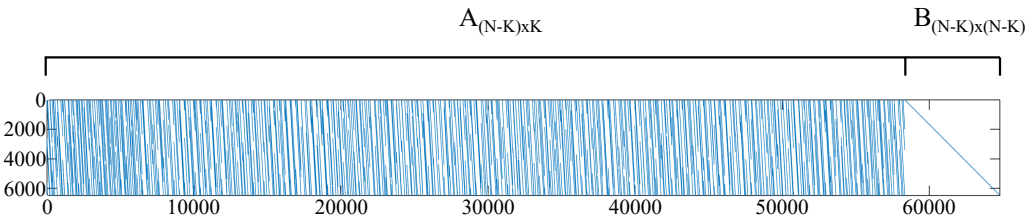


Figure 5.2: **Parity-check matrix.** Shown is a parity check matrix $H_{(N-K)\times N}$ used to encode bit strings of length $K = 58320$ into codewords of $N = 64800$ bits. The blue and white dots encode the bit 1 and 0 respectively. The matrix shown here is provided by the DVB-S2 standard for a code rate $r = K/N = 0.9$.

binary search on the first half. If no errors are found they check the second half until the error is found and corrected.

6. Repeat from step 1 with block size $2k$.

At the end of the protocol Alice and Bob hold the same key, which however has been partially revealed during the sharing of the parity bits. Note that the choice of the block size is critical, as too large blocks would likely contain two errors which thus will not be accounted for in the parity. However, if the blocks are too small, the amount of information disclosed to Eve would be maximal. Note that the initial size k is a free parameter, and must depend on QBER. The analytical dependence is not known but it was shown in [138] numerically that the value $k \approx \frac{0.73}{\text{QBER}}$ is optimal.

5.2.2 Low-Density Parity-Check Codes

Low-density parity-check (LDPC) codes [139] are a fundamental component in classical error correction theory, and are employed nowadays for satellite transmission of digital signal as specified in the DVB-S2 standard [140, 141]. LDPC codes belong to the one-way EC approach, and they found an application for long-distance QKD [142] where the two-way codes such as Cascade are unpractical due to large latency and communication overhead required to minimize the information leakage to Eve [143, 144]. The main limitation to an extensive use of these codes in QKD is however their computational complexity, primarily affecting the key rate [145].

We describe now the working principle of LDPC codes following the notation of the DVB-S2 standard described in [140]. The choice of focussing on the DVB-S2 standard is motivated by the fact that we will use it for our conference key agreement results, which will be shown in the following sections. LDPC codes encode a blocks

of K bits $(i_0, i_1, ..., i_{k-1})$ into codewords c of N bits $(i_0, i_1, ..., i_{k-1}, p_0, p_1, ..., p_{n-k-1})$ by means of a parity-check matrix $H_{(N-K)\times N}$. The encoding is obtained by imposing $Hc^T = 0$ and solving with respect to the parity bits $(p_0, p_1, ..., p_{n-k-1})$. In particular, the form of the parity-check matrix is assumed[1] to be [140, 141], $H_{(N-K)\times N} = A_{(N-K)\times K} B_{(N-K)\times(N-K)}$ where B is a staircase lower triangular matrix see Fig 5.2. With this assumption, the complexity of the encoding is reduced to a linear complexity and the parity bits are obtained by recursively solving

$$H_{00} i_0 + ... + H_{0,K-1} i_K + p_0 = 0$$

$$H_{10} i_0 + ... + H_{1,K-1} i_K + p_0 + p_1 = 0$$

$$\vdots$$

$$H_{N-K-1,0} i_0 + ... + H_{N-K-1,K-1} i_K + p_{N-K-2} + p_{N-K-1} = 0$$

In classical EC the entire codeword $(i_0, i_1, ..., i_{k-1}, p_0, p_1, ..., p_{n-k-1})$ is sent to the receiver for decoding and correction of the bit-flip errors occurring in the classical transmission channel. In QKD this can not be the case and only the parity bits $(p_0, p_1, ..., p_{n-k-1})$ are sent to Bob. An important figure of merit is the code rate defined as $r = K/N$ which in principle can be any number from 0 to 1 and it depends on the value of the QBER according to

$$r = 1 - h(\text{QBER}). \tag{5.2}$$

Note that as in the DVB-S2 standard the codewords are fixed to $N = 64800$ the value of QBER sets through the code rate the number of parity bits which Alice has to send. Of course, the higher is the QBER the lower is the code rate increasing the amount of information leaked to Eve.

The decoding takes as input Bob's codeword $(i'_0, i'_1, ..., i'_{k-1}, p_0, p_1, ..., p_{n-k-1})$ where $(i'_0, i'_1, ..., i'_{k-1})$ are Bob's raw bits to be corrected and $(p_0, p_1, ..., p_{n-k-1})$ are Alice's parity-check bits. In essence, the idea for the decoding is the following: Bob

[1] As explained in [140] this assumption leads to negligible (within 0.1 dB) performance loss with respect to a general parity-check matrix.

assigns to each raw bit i'_0 a random variable $y = x + z$, where z is a Gaussian random variable with zero mean and x is the value of Alice's original bit i_0. We assume that $x = +1$ if $i_0 = 0$ and $x = -1$ if $i_0 = 1$ and build a log-likelihood variable u,

$$u = \log \frac{p(x = +1|y)}{p(x = -1|y)}. \tag{5.3}$$

Thus, the sign of u indicates whether Alice's bit and Bob's bit are the same or not, whereas the amplitude of u will indicate how likely that is the case i.e. the bigger is the magnitude, the higher is the reliability. The idea is to start with *a priori* value of u and then update it according to the information contained in the parity-check bits until a high amplitude of u is reached. Finally, according to the sign of u, Bob will flip his bit or leave it unchanged. For a more detailed description of the decoding algorithm the reader is referred to Ref. [140]. Notably, LDPC codes can reach an efficiency close to the Shannon limit in the asymptotic case of large block size K but at cost of exploding dimension of parity-check matrices and increasing complexity of the decoding algorithm. Nevertheless, it was shown in [143] how optimized LDPC codes can perform better than Cascade as soon as the error rate is above 2%.

5.3 Conference Key Agreement

We have described so far all the different aspects of the paradigmatic 2-party QKD, where only Alice and Bob want to share a secret and common key. However, it is reasonable to assume that in future practical implementations more parties will be involved and a secret conference key distributed to them.

Conference key agreement is a multi-user protocol for sharing a common information-theoretic secure key [146], allowing a group of authenticated users to communicate securely, wherein exclusively members of the group can decrypt messages broadcast by any other member. One approach to distribute a conference key is to iterate two-party QKD (2QKD) primitives to establish secret keys between pairs of users in the group, followed by an additional bitwise XOR operation per pair of users transforming the unique keys into a common secret key [147, 148]. An alternative approach is to share genuine multi-partite GHZ entangled states [149, 150] between users of the group, enabling the direct extraction of the conference key without

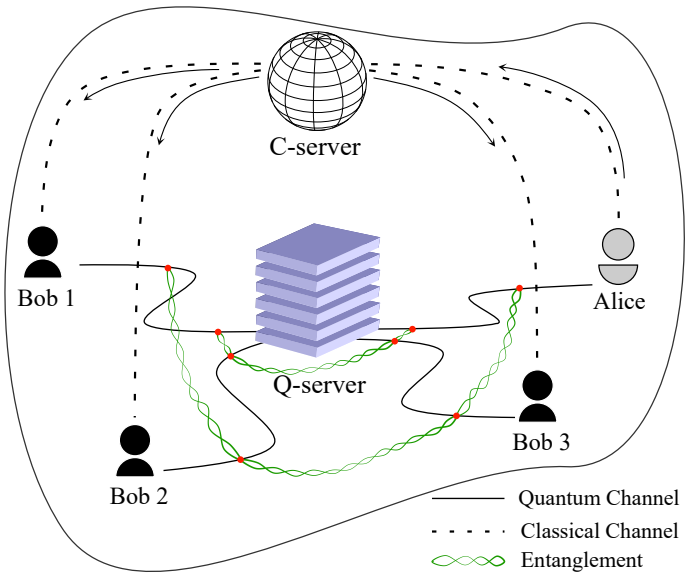


Figure 5.3: **Four party quantum conference key agreement.** A quantum server (Q-server) distributes entangled GHZ states to four parties Alice, Bob 1, 2, and 3. They communicate through an authenticated classical channel (C-server) to establish a common secure key from a sequence of local measurements.

requiring any additional step (see Fig. 5.3).

In this section we outline the steps of the N-BB84 protocol for conference-key recently introduced by *Grasselli et al.* [149].

1. An untrusted quantum server prepares and distributes for L rounds the maximally entangled GHZ state, $|GHZ\rangle \equiv (|0\rangle^{\otimes N} + |1\rangle^{\otimes N})/\sqrt{2}$, to N participants in the network.
2. Each user performs local quantum measurements on their respective qubit in either the Z-basis constituting type-1 rounds, or the X-basis for type-2 rounds. Type-2 rounds are carried out randomly with probability p, for a total of $m = L \cdot p$ rounds. Users coordinate the measurement sequence using $L \cdot h(p)$ bits of a pre-shared key.
3. Once the measurements are performed, users proceed to verify the security of their key by performing parameter estimation. All users announce their outcomes for a subset of the type-1 rounds, m in total and randomly chosen, and all m type-2 rounds to determine $Q^m_{\mathrm{AB}_i} = \left(1 - \langle \sigma_z^{\mathrm{A}} \sigma_z^{\mathrm{B}_i} \rangle\right)/2$ for $i = \{1, 2, ..., N\}$ and $Q^m_X = \left(1 - \langle \sigma_x^{\otimes N} \rangle\right)/2$ respectively. We define the quantum bit error rate (QBER) as $\mathrm{QBER}^m \doteq \max Q^m_{\mathrm{AB}_i}$.
4. All users retain $n = L - 2m$ bits forming the raw conference key, subsequently

corrected with an error correction scheme and shortened with privacy amplification to ensure security.

5. Finally, all users remove $L \cdot h(p)$ bits from their secret conference key to encode the pre-shared keys for subsequent protocols.

Notably, owing to the structure of the GHZ state, type-1 rounds are used to obtain the raw key as these measurements ensure all users in the protocol obtain the same bit value. Type-2 measurements instead are used to detect the presence of an eavesdropper. As outlined above, the order of the type-1 and type-2 measurements is set by a pre-shared key. In particular, one user generates the L-bit string indicating the measurement type of each round. The string can be classically compressed, shared, and decompressed by the other parties. Note that the values of p are typically on the order of 0.02, leading to a small value of $h(p)$, i.e., the amount of information to be initially pre-shared is small. Hence, the protocol is a key-growing routine, as in any known QKD scheme. Conversely from 2QKD schemes, during EC, $N-1$ raw keys should be corrected. In this new multi-party scenario, choosing one-way or two-way error correction might be of primary importance. In fact, a preliminary study[2], suggests that one-way EC codes are the only sensible option already starting with three users. In fact, for QBER $\gtrapprox 0.55\%$, they outperform the two-way approach based on the CASCADE protocol iterated for all the Alice-Bob$_i$ pairs.

Finally, for privacy amplification, one user sends information for a two-universal hash function, i.e., the first row and first column of a Toeplitz matrix [151], to all users who apply it to their corrected keys to obtain a shortened secure conference key. In particular, the maximal probability that a potential eavesdropper holds at least some information about the established key after the PA step should be lower than a given security parameter ϵ_{tot}, which as we will see is typically on the order of $10^{-}8$.

5.3.1 Conference Key in the Asymptotic Limit

We consider here the limit of $L \to \infty$. In this asymptotic regime nearly all rounds are used to extract the raw key and we define the asymptotic key rate (AKR) as

[2]By Krzysztof Skrzypczak, a master student working in our group, who numerically simulated a comparison between LDPC codes and Cascade in a multi-party scenario.

the fraction of secret bits ℓ, extracted from the total rounds [149] as given by:

$$\mathrm{AKR} = \frac{\ell}{L} = 1 - h(Q_X) - h(\mathrm{QBER})\,, \tag{5.4}$$

where $h(x)$ is the Shannon entropy [131]. Note that here, Q_X and QBER take the operational meaning of probabilities derived from the frequencies Q_X^m and QBER^m in the limit of $m \to \infty$ although $p \to 0$. This limit should be seen as an upper bound to any realistic implementation of the protocol, where instead finite-key effects contribute to the achievable key rate as shown in the next section.

5.3.2 Finite-key Effects

When performing the N-BB84 protocol in practice, only a finite number of rounds L is available. In this regime, the estimated parameters Q_X^m and QBER^m from the m type-2 and type-1 rounds, are affected by statistical error which must be taken into account in the final key rate. The fractional key rate in this case is given by [149],

$$\begin{aligned}\frac{\ell}{L} = \frac{n}{L}[1 - h(Q_X^m + 2\xi_X) - h(\mathrm{QBER}^m + 2\xi_Z)] - \\ - \log_2\left[\frac{2(N-1)}{\epsilon_{EC}}\right]^{\frac{1}{L}} - 2\log_2\left[\frac{1-2(N-1)\epsilon_{PE}}{2\epsilon_{PA}}\right]^{\frac{1}{L}} - h(p)\,,\end{aligned} \tag{5.5}$$

where N is number of users in the protocol, (ξ_X, ξ_Z) are finite-key correction terms and $(\epsilon_{EC}, \epsilon_{PE}, \epsilon_{PA})$ set the security parameters of the protocol. In particular, in the finite-key scenario, Alice needs to set the length of the privacy amplification output to Eq. (5.5) in order to ensure that the established key is secure with security parameter ϵ_{tot}. The security parameter ϵ_{tot} represents the maximal probability that a potential eavesdropper gains at least some information about the established key. It is related to the failure probabilities of the different stages of the protocol as follows: $\epsilon_{tot} = \epsilon_{EC} + \epsilon_{PA} + 2\epsilon_{PE}$, where ϵ_{EC} is the maximal failure probability of the error correction procedure and ϵ_{PA} represents the same in the case of privacy amplification, while the last term is related to the failure probability of the parameter estimation step. In particular, the observed values QBER^m and Q_X^m in the $2m$ rounds devoted to PE might differ from the corresponding values QBER^n and Q_X^n characterizing the remaining $n = L - 2m$ rounds which are used to extract the

secret key. The deviation of QBER^n and Q_X^n is quantified by the theory of random sampling without replacement [152] and must be accounted for in the secret key rate Eq. (5.5), by taking the worst-case in order to preserve security. As shown in Ref. [149], the distance $|\mathrm{QBER}^n - \mathrm{QBER}^m|$ ($|Q_X^n - Q_X^m|$) between the pairwise bit discordance (the parameter Q_X^n) and its observed value is not larger than $2\xi_Z$ ($2\xi_X$) with probability at least $1-\epsilon_Z$ ($1-\epsilon_X$), where:

$$\xi_{Z,X} = \sqrt{\frac{(n+m)(m+1)}{8nm^2} \ln\left(\frac{1}{\epsilon_{Z,X}}\right)} \ . \tag{5.6}$$

By combining the above statements one can deduce that:

$$\begin{aligned} &\Pr\left[Q_X^n \leq Q_X^m + 2\xi_X \ \wedge \ Q_{AB_i}^n \leq Q_{AB_i}^m + 2\xi_Z \ \forall i\right] \\ &\geq 1 - \epsilon_{PE}^2 \ , \end{aligned} \tag{5.7}$$

where we defined the total parameter estimation failure probability ϵ_{PE}^2 as follows:

$$\epsilon_{PE}^2 \equiv (N-1)\epsilon_Z + \epsilon_X \ . \tag{5.8}$$

Note that the probabilities ϵ_Z and ϵ_X, and hence ϵ_{PE}^2, can be chosen freely as to maximize the resulting secret key rate, with the only constraint that: $\epsilon_{PE} \leq \epsilon_{tot}$. The maximization of the equation (5.5) determines the value of p to be used during the protocol. As we will see, this is typically of the order of 0.02 for values of QBER^m and Q_X^m lower than 0.05.

5.4 Experimental N-BB84 Protocol

In this section the first experimental demonstration of the N-BB84 protocol is presented. The protocol is performed in a four-party scenario consisting of: Alice (A), Bob 1 (B_1), Bob 2 (B_2), and Bob 3 (B_3). Experimentally, the required 4-qubit GHZ state is implemented in a photonic platform where single photons are employed to encode qubits. After the state is prepared, it is distributed to the four parties by means of single mode fibres of variable length. In particular we fix Alice's channel

at 2 m from the server whereas we employ fibres of length d_i (in kilometres) between B_i and the server. The topology is denoted as $\{d_1, d_2, d_3\}$ for B_1, B_2 and B_3 respectively. The experimental setup is described in detail in the next subsection.

5.4.1 Experimental Setup

The employed experimental setup has strong similarities with the one already described in Chapter 4, Section 4.4, and the reader is pointed to Chapter 3 for further details on the main components. Single photons produced from type-II collinear spontaneous parametric down-conversion in a 22 mm long PPKTP crystal, are employed to implement qubits with the encoding $|h\rangle \equiv |0\rangle$ and $|v\rangle \equiv |1\rangle$. The PPKTP crystals are embedded within a polarisation-based Sagnac interferometer [46] and pumped bidirectionally, using a half-wave plate to set diagonally-polarised light, to create polarisation-entangled photons at 1549.8 nm in the state:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}} \left(|h\rangle|v\rangle - |v\rangle|h\rangle\right), \tag{5.9}$$

which we can map to any Bell state via local operation on one of the two photons. We note that at the chosen wavelength the typical fibre loss is 0.2 dB per km. As show in Fig. 5.4 two of these sources are employed, they are pumped using a mode-locked laser operating with a nominal repetition rate of 80 MHz, 1.4 ps pulses and its central wavelength at 774.9 nm. A passive pulse interleaver is used to quadruple the 80 MHz pulse train to 320 MHz [153]. With loose bandpass filters of 3 nm bandwidth, we measure an average source brightness of ~ 4100 pairs/mW/s, with a symmetric heralding efficiency of $\sim 60\%$. The average heralding efficiency reduces by $\sim 12\%$ with a commensurate decrease of 45% in source brightness at the point of detection of the four users at zero distance. We characterise each photon pair source by performing quantum state tomography, reconstructing density matrices using maximum-likelihood estimation and Monte-Carlo simulations based on Poissonian count statistics to determine errors. For each source we obtain a typical two-photon Bell-state fidelity $F = 95.58 \pm 0.15\%$ and purity $P = 92.07 \pm 0.27\%$, while entanglement is measured by concurrence $\mathcal{C} = 92.38 \pm 0.21\%$.

The four-photon GHZ state is created by interfering one photon from each source

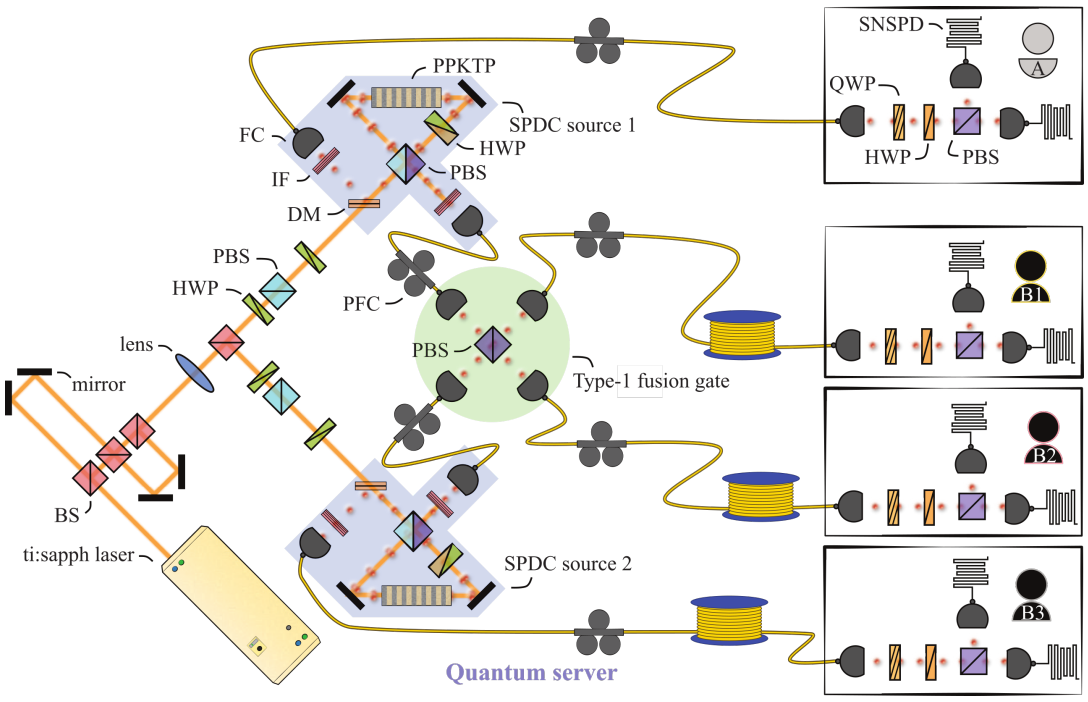


Figure 5.4: **Experimental conference key agreement setup.** A mode-locked picosecond laser (ti:sapph) multiplexed to 320 MHz repetition rate supplies two entangled photon sources producing polarisation-entangled Bell pairs. Down-converted photons are separated from the pump with dichroic mirrors (DM) and coupled into fibres (FC). One photon from each source non-classically interfere on a polarising beamsplitter (PBS) creating the four-photon GHZ state. Each user receives their photon via single-mode fibres and performs projective measurements in the Z(X) basis by using a quarter- (QWP) and half-wave plate (HWP), and a polarising beamsplitter (PBS) before detection with superconducting nanowire single-photon detectors.

on a polarising beamsplitter (PBS), which transmits horizontally and reflects vertically polarised photons. Post-selecting on the case where one photon is emitted in each output, which occurs with a probability of 1/2, we obtain the state

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|hhhh\rangle - |vvvv\rangle\right) , \tag{5.10}$$

We measure independent two-photon interference visibility of $92.96 \pm 0.95\%$ using 100 mW pump power, and four-qubit state tomography returns a purity and fidelity of $P = 81.39 \pm 0.83\%$ and $F = 87.58 \pm 0.48\%$ respectively.

Each user receives their photon via single-mode fibres and performs projective measurements in either the Z-basis for type-1 measurements or X-basis for type-2 measurements, as prescribed by the pre-shared key. The measurements are realised by using a sequence of a quarter-wave plate, half-wave plate and a polarising

beamsplitter before detection with superconducting nanowire single-photon detectors with nominal detection efficiency of $\approx 80\%$. Detection events are time-tagged and counted in coincidence within a 1 ns time window.

5.5 Results

We report here the experimental results demonstrating the feasibility of the conference key agreement protocol under study. The results are divided in two parts, firstly we present the results achieved assuming an infinite number of rounds. This is done in several network topologies and the key rates determined by Eq. (5.4). The second part, which we could consider as the main result, is a thorough experimental study in the finite-key regime as governed by Eq. (5.5). From a finite number of rounds, a secret conference key is extracted following EC and PA.

5.5.1 Key rates in the asymptotic limit

From Eq. 5.4 we note the AKR depends only on the noise parameters Q_X and QBER. We estimate these parameters experimentally using a large sample size of type-1 and type-2 measurements to minimise uncertainties. We implement four scenarios: $\{0, 0, 0\}$, $\{0, 0, 20\}$, $\{0, 10, 20\}$, and $\{20, 10, 20\}$, corresponding to measured network losses (in dB) of 0, 4.84, 7.57, and 11.77. The observed four-photon generation rates g_R for these scenarios are 40.89 Hz, 12.68 Hz, 6.31 Hz, and 2.03 Hz. The conference key rate is determined as a product of the fractional AKR and the recorded generation rates g_R. The results are shown in Fig. 5.5. In all cases we observe similar noise parameters, and thus AKRs, indicating that the entanglement quality is not degraded significantly by the transmission fibres.

The experimental value of the AKR is mainly limited by multiple-pair generations at the sources and by spectral impurities of the photons. Qualitatively, the multiple-pair generations at the source will mainly effect the value of the QBER whereas the coherence of the GHZ and thus the Q_X is mainly degraded by imperfect spectral mode-matching at the PBS. In fact, as observed in Fig. 5.6, the QBER can be tuned by changing the pump power, and in the limit of very low powers the QBER tends to the ideal value of 0. The same effect is not true for Q_X which mostly

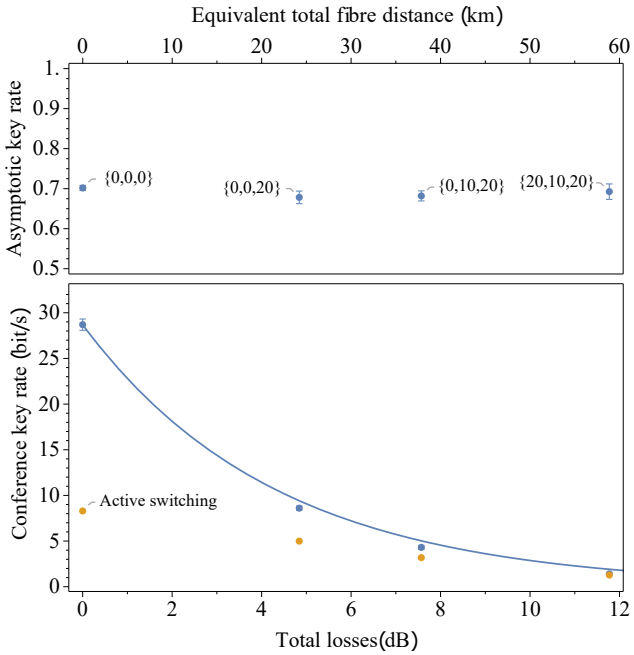


Figure 5.5: **Asymptotic key rate results**. (top) We determine the fractional asymptotic key rate (AKR) by measuring Q_X and QBER without performing the full protocol. We evaluate AKR for a range of loss conditions set by the placement of fibre links in the network. (bottom) The conference key rate is plotted as a function of the total fibre length in the network. We include results of the generation rates with measurement-basis switching using our implementation.

depends on the amount of coherence in the experimental GHZ state and therefore on the indistinguishability of the interfering photons at the PBS in all the degrees of freedom, i.e.: polarisation, photon-number, time and spectrum. In particular, although our photons are spectrally filtered at the source, they retain some spectral mixture intrinsic to the PDC process giving a lower bound for the measurable Q_X. Such lower bound can be linked to the experimentally measured visibility as follows. Assuming that the photons at the PBS successfully interfere with some probability t, we can write the state ρ_o after the interference as:

$$\rho_o = t\rho_s + (1-t)\rho_f. \tag{5.11}$$

Where ρ_s is the density matrix of the state in case of success, given by $\rho_s = |\text{GHZ}\rangle\langle\text{GHZ}|$, and ρ_f is the density matrix in case of failure given by $(|hhhh\rangle\langle hhhh| + |vvvv\rangle\langle vvvv|)/2$. The expected Q_X for this state is

$$Q_X = \frac{1 - \text{Tr}\left[\rho_o \otimes X^{\otimes 4}\right]}{2} = \frac{1-t}{2}. \tag{5.12}$$

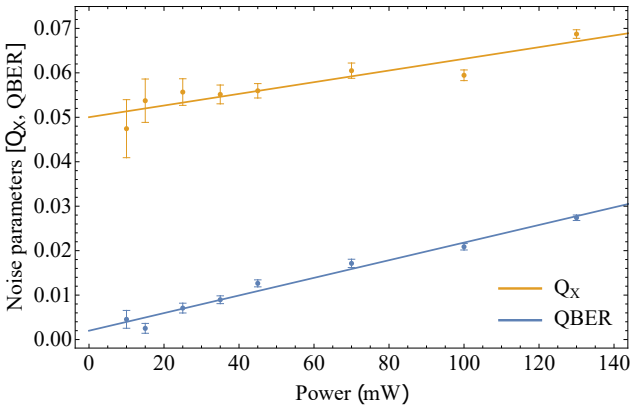


Figure 5.6: Q_X **and QBER as a function of power.** Shown are the values of the two parameters as a function of the pump power, therefore varying the probability for multi-pair generations in the photon sources. Within the range of power considered, the trend is linear although the slope for the QBER is greater than the slope for Q_X. Moreover, Q_X is lower-bounded by the value of 0.05 at zero power.

Note that for $t = 1$, $Q_X = 0$, and for $t = 0$, $Q_X = 1/2$. Similarly, given the experimentally measured visibility V_{exp} we expect $Q_X = 0$ and $Q_X = 1/2$ for $V_{\text{exp}} = 1$ and $V_{\text{exp}} = 0$ respectively. We can thus, at least for these two extreme cases, interpret t as V_{exp}. Assuming that $t \approx V_{\text{exp}}$ in general, we have that for $V_{\text{exp}} = 0.9$, $Q_X = 0.05$ in accordance with our results. It should be noted however, that the interference at the PBS is a coherent process, which might not be fully characterised by the simple model just presented. Hence, in general, we can conclude that $Q_X \gtrsim (1 - V_{\text{exp}})/2$.

5.5.2 Active Switching

Most QKD protocols require random switching of the measurement basis, either passively or actively, with each clock cycle. The same holds for the N-BB84 protocol, where users switch between the Z/X measurement bases according to a pre-shared random sequence.

As noted, p is typically small hence switching between bases occurs relatively infrequently. In addition the multi-photon detection rates in our experiment are low, hence the standard method of polarisation switching with electro-optic modulators would be excessive. We therefore implemented active switching using motorised rotation stages with switching speeds on the order of seconds—marginally slower than our average required switching periods, which reduces the maximum possible raw generation rate g_R.

Assuming a switching time τ_s i.e. the time required for the plates to move from one setting to another, we have a number $g_R\tau_s$ of undetected events. Therefore if without switching and measuring for T seconds we have a total number of events $g_R T$, when we introduce a switch with probability p the number of total events is $g'_R T = (1-p)g_R T - p g_R \tau_s$ from which we obtain

$$\frac{g'_R}{g_R} = (1-p) + p\frac{\tau_s}{T}. \tag{5.13}$$

We evaluate the adjusted generation rate g'_R for the finite key scenario for the $\{5, 10, 20\}$ topology, by performing 1000 rounds of the protocol with active basis switching. We set $p = 0.02$, thus 20 type-2 rounds are randomly allocated in the measurement sequence. We measured the reduced key generation rate and found $g'_R/g_R = 0.91$, from which we obtain τ_s and use Eq. (5.13) to extrapolate the adjusted generation rates obtained in the asymptotic case as shown by orange dots in Fig. 5.5.

5.5.3 Active Polarisation Control

The optical fibre links in our experiment are realised by spools of bare SMF28 fibre. Thermal drifts in the laboratory introduce unwanted rotations in polarisation which, if uncorrected, lead to added noise in the protocol. This effect was mitigated passively by enclosing the bare fibres in a polystyrene box, and actively with a feed-forward polarisation control as explained in the following. In general propagation in fibre introduces both non-linear and linear effects. For polarisation-encoded single photons, the former effect can lead to dephasing between the horizontal and vertical components of the polarisation. This effect known as polarisation mode dispersion is negligible in our case as at telecom wavelength becomes important for distances starting from thousands of kilometres [154]. Linear effects, include unitary rotations of the polarisation which can be in principle completely undone. Unfortunately, our setup only allows to measure the action of the fibres on the Z-basis and full correction is not possible. Nevertheless, as the QBER only depends on the measure of the GHZ state in the Z-basis, a partial correction can introduce improvement and is implemented as follows. Recalling Fig 5.4, consider for instance the fibre

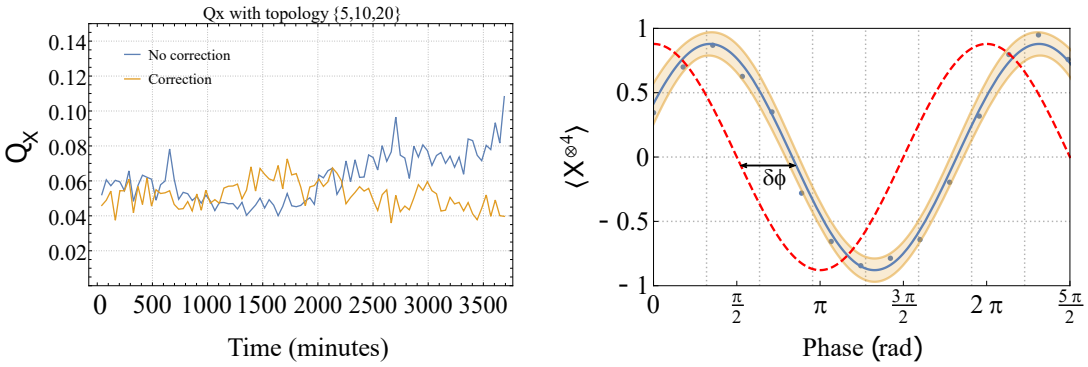


Figure 5.7: **Effect of fibres on Q_X** The change of the Q_X value is measured over time and the effect of active correction (in orange) is compared to the case without any correction (blue). The correction consists in finding the phase mismatch in the X-basis. This is achieved by applying the local unitary $U = |h\rangle\langle h| + e^{i\delta\phi}|v\rangle\langle v|$ on Alice and extrapolating $\delta\phi$ from the difference of the observed fringes (blue dots and blue fit) and the expected trend in dashed-red for an ideal 4-GHZ.

channel on Bob 1. As source 1 creates the entangled state $|\psi^-\rangle$, upon heralding of an $|h\rangle$ photon on Alice's detection stage, the second photon is steered into the state $|v\rangle$ which is therefore reflected by the PBS and sent through the fibre before arriving in Bob1's detection stage. There, the single-qubit expectation values of σ_x, σ_y and σ_z are evaluated enabling in post-processing the reconstruction of the single-qubit density matrix and the effective rotation in the Z-basis induced by the fibre. The HWP and QWP settings are therefore updated in order to undo the unwanted rotation i.e. the states $|h\rangle$ and $|v\rangle$ are unchanged by the fibre. The whole procedure takes 30 seconds, and is performed simultaneously for all the fibre-channels preserving the populations of the global 4-qubit GHZ state (but not their coherence) and thus the low QBER. The method was tested by measuring for almost three consecutive days the GHZ states in the Z-basis and comparing the Q_{AB_i} of the three Bobs with and without the active feedback. As shown in Fig. 5.8 the effects are typically negligible for short fibre lengths, e.g., in our testing we found the 5 km spool added no observable noise greater than with a 2 m fibre link, while the 10 km and 20 km spools showed significant added noise in $Q_{\mathrm{AB}i}$ measurements if not corrected. During the experiment, we implement active polarisation control to correct for these effects during key transmission to preserve low-noise operation throughout the protocol once every $\sim$ 20 minutes for an optimal tradeoff between maintaining a high duty-cycle while minimising bit error rates.

As mentioned before, the main limitation of the method is that despite the errors

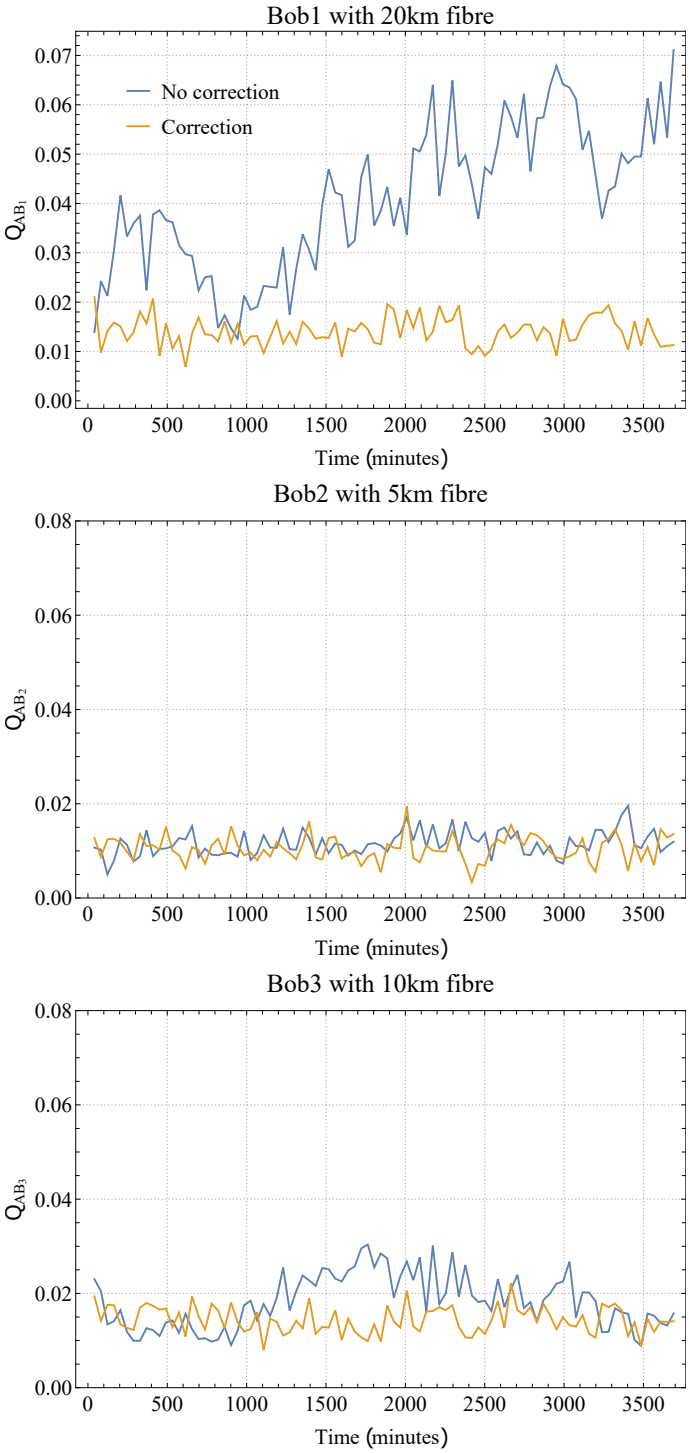


Figure 5.8: **Z-basis active correction.** Shown is the effect on the QBER due to unitary rotations introduced by the fibre channel over time. The effect is shown for B_1, B_2 and B_3 (from top to bottom) with (orange) and without (blue) the active feedback. This is operated actively by performing single-qubit tomography every 41 minutes on each user to estimate the Z-basis rotation introduced by the fibre. A new reference frame is then set by adjusting QWP and HWP angles such that the QBER is minimized. Notably, the feedback is crucial for B_1 where a 20 km fibre is employed.

being fully corrected in the Z-basis, they are not in the X-basis which determines the value of Q_X. This is accounted by performing 4-qubit phase estimation before type-2 measurements, in fact the coherence of the global 4-GHZ state can be controlled by a local unitary on one of the qubits (in our experiment Alice's qubit). The phase estimation permits the evaluation of the phase mismatch $\delta\phi$ and its correction by scanning the Alice's HWP angles and recording the 4-fold coincidences. As shown in Fig. 5.7, the interference fringes obtained in post-selection will show a phase-shift respect to the reference phase which can thus be matched back by simple Alice's HWP rotation. In the experiment, this procedure takes no more than 5 minutes, however is worth to note that in general such approach is highly-inefficient as requires 4-fold coincidences and relatively long run-time.

5.5.4 Finite-key Results

When operating with a finite number of rounds, the value of p i.e. the probability of a type-2 measurement has to be evaluated. In the experiment, we set the required security parameter to $\epsilon_{tot} = 1.8 \times 10^{-8}$ and obtained preliminary estimations for QBER $= 0.02$ and $Q_X = 0.05$. Then Eq. (5.5) is maximised over the failure probabilities $\epsilon_Z, \epsilon_X, \epsilon_{EC}$ and ϵ_{PA} and over the fraction of type-2 rounds p. We obtain optimal values: $p = 0.012$, $\epsilon_{EC} \sim 10^{-13}$ and $\epsilon_{PA} \sim 10^{-10}$. With this value of p, the amount of information reserved for the pre-shared key is $h(p) = 0.093$. For the experiment, the topology is fixed to $\{5, 10, 20\}$ with a measured loss of 9.53 dB in total.

We obtain over 4.09×10^6 type-1 rounds and 5.01×10^4 type-2 rounds during 177 hours of continuous measurement. We implement one-way error correction using LDPC codes complying with the Digital Video Broadcasting (DVB-S2) standard [141]. The codes used in the experiment have been modified from the MATLAB communication package based on the DVB-S2 standard [141], and adapted to our multi-party scenario, simultaneously correcting Bob 1, Bob 2, and Bob 3 keys. In the experiment, we set the code rate according to the estimated QBER using m samples with appropriate ξ_Z correction. From the provided set of code rates we used 1/2, 1/3 and 1/4 for small, mid and large values of L as shown in Fig 5.9a. Alice uses the parity matrix to calculate the parity check bits to send them together

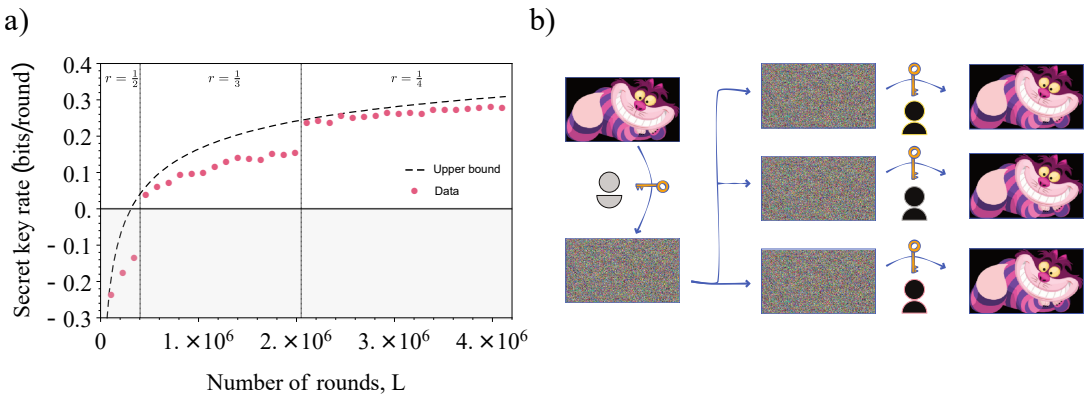


Figure 5.9: **a) Finite key results**. We implement all steps in the N-BB84 protocol for a range of L rounds to retrieve the final key of length ℓ and evaluate the secret key rate, $SKR = \ell/L$. The upper bound given by Eq. 5.5 is shown compared with the experimental data. **b) Encryption**. We generate an ϵ_{tot}-secure conference key of 1.15×10^6 bits. Using 1.06×10^6 bits, Alice encrypts an image (8-bit RGB, 280 by 158 pixels) employing a one-time-pad scheme. Alice sends the encrypted image over a public channel allowing only Bob 1, Bob 2, and Bob 3, who share the conference key, to decode the image.

with the H matrix, to all parties through an authenticated classical channel. Each Bob implements a decoding algorithm consisting of simple addition, comparison and table look-up operations.

EC ensures that all parties share a common key, however it remains partially secret owing to information leaked during error correction, and any potential eavesdropping during the distribution step. In order to reduce the information held by any potential eavesdropper, we implement one round of privacy amplification on the entire raw key, reducing its final length. We use Toeplitz matrices for this purpose, a class of universal-2 hash functions [155] that can be implemented efficiently for our given key size.

We estimate the theoretical performance of our post-processing steps by evaluating the noise parameters $Q_X = 0.05$ and QBER $= 0.0159$, which we use to calculate the upper bound set by Eq. (5.5) and plotted in Fig 5.9 a (dashed line). When performing the protocol in earnest with a finite data set to estimate these parameters, we replace the Shannon limit for the error correction term $h(\text{QBER}^m + 2\xi_z)$ in Eq. (5.5) with the fraction of parity bits disclosed by Alice.

In conclusion, we generate an ϵ_{tot}-secure conference key of 1.15×10^6 bits. Using 1.06×10^6 bits, Alice encrypts an image of a Cheshire cat (8-bit RGB, 280 by 158 pixels) employing a one-time-pad scheme. Alice sends the encrypted image over a

public channel allowing only Bob 1, Bob 2, and Bob 3, who share the conference key, to decode the image.

5.6 Topology Dependence for Conference Key Rates

Before moving to the end of the chapter, is worth to discuss a problem absent in the standard Alice-Bob scenario. Since conference key protocols are performed over a network where different users are connected according to some topology, the conference key rates might in general depend on the noise distribution in the network. Here, we study for simplicity a 3-party scenario composed by Bob 1, Bob 2 and Bob 3 all independently connected to one common server, with the noise affecting each link modelled as a depolarising channel

$$\mathcal{D}(\rho) = (1 - \frac{3p}{4})\mathcal{I} + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z). \tag{5.14}$$

In general, the channels of Bob 1, Bob 2 and Bob 3 are described by the noise parameters p_{B1}, p_{B2}, and p_{B3}, respectively. We consider the expressions of Q_X and Q_{ABi}, for a depolarised 3-qubit GHZ state with noise parameters p_{B1}, p_{B2} and p_{B3}, are

$$Q_X(p_{\mathrm{B1}}, p_{\mathrm{B2}}, p_{\mathrm{B3}}) = \frac{[(p_{\mathrm{B1}} - 1)\,(p_{\mathrm{B2}} - 1)\,(p_{\mathrm{B3}} - 1) + 1]}{2} \tag{5.15}$$

$$Q_{ABi}(p_{\mathrm{Bi}}) = \frac{p_{\mathrm{Bi}}}{2} \tag{5.16}$$

Q_X depends on the noise parameters of all the channels, whereas Q_{ABi} only depends locally on the noise parameter affecting the link connecting Alice and B_i. Of course, both functions have a global minimum in $(p_{\mathrm{B1}}, p_{\mathrm{B2}}, p_{\mathrm{B3}}) = (0, 0, 0)$, that is when all the channels are noiseless.

What is interesting to study is whether both functions have a minimum with the constraint $p_{\mathrm{B1}} + p_{\mathrm{B2}} + p_{\mathrm{B3}} = c$ where c is a constant in the interval $c \in [0, 3]$. In practice, this corresponds to fix some total amount of noise strength c on the network and finding which solution gives the highest key rate i.e. the lowest Q_X and Q_{ABi}. It is straightforward to see that the minimum of $\max_i Q_{ABi}$ is given by

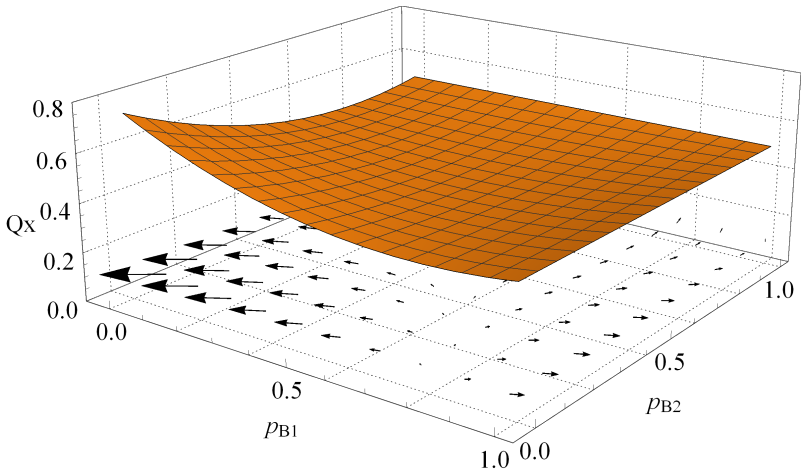


Figure 5.10: **Conference key rates under depolarizing noise.** Shown is the Q_X as a function of the noise parameters p_{B1} and p_{B2} characterising the depolarising channels (Eq. 5.15) of Bob 1 and Bob 2, respectively. The noise parameter of Bob 3 is fixed to: $p_{B3} = 1.5 - p_{B1} - p_{B2}$. We also insert the vector field of the gradient of Q_X with respect to p_{B1} and p_{B2}.

$p_{\mathrm{B1}} = p_{\mathrm{B2}} = p_{\mathrm{B3}} = c/3$. To find the minimum of Q_X, we compute the gradient of $f(p_{\mathrm{B1}}, p_{\mathrm{B2}}) = Q_X(p_{\mathrm{B1}}, p_{\mathrm{B2}}, c - p_{\mathrm{B1}} - p_{\mathrm{B2}})$

$$\frac{\partial f(p_{\mathrm{B1}}, p_{\mathrm{B2}})}{\partial p_{\mathrm{B1}}} = \frac{1}{2}(p_{\mathrm{B2}} - 1)(c - 2p_{\mathrm{B1}} - p_{\mathrm{B2}})) \tag{5.17}$$

$$\frac{\partial f(p_{\mathrm{B1}}, p_{\mathrm{B2}})}{\partial p_{\mathrm{B2}}} = \frac{1}{2}(p_{\mathrm{B1}} - 1)(c - p_{\mathrm{B1}} - 2p_{\mathrm{B2}})) \tag{5.18}$$

The plot in Fig. 5.10 shows the function $f(p_{\mathrm{B1}}, p_{\mathrm{B2}})$ for $c = 1.5$ with at the bottom the vector field of the gradient as given by ∇f. One can verify that the minimum of the function is in $p_{\mathrm{B1}} = p_{\mathrm{B2}} = p_{\mathrm{B3}} = c/3$, therefore we conclude that the maximum conference key rate is achievable when the noise is symmetrically spread over the network. This result intuitively reflects the symmetry of the GHZ state, however in practice we can never assume the same amount of noise in all the channels. Nevertheless, as the function is quite flat around the minimum, the effect on the key rate could be neglected for small deviations from the symmetric configuration.

5.7 Discussion and Conclusions

The security of the N-BB84 protocol is based on the proof in [149] and the assumptions therein. In the security proof only Alice's measurement device is trusted

whereas Bobs' measurement devices can be untrusted. More precisely Alice's measurement device should be trusted to indeed realise the type-1 and type-2 measurement settings as prescribed by the protocol. We ensure this condition is met by full characterisation of the measurement stages prior to the experimental run. Adapting the quantum conference-key agreement protocol for full (measurement-)device-independence is a work in progress, see for example [156, 157].

Experimental 2QKD key rates are bounded by the the well-known repeaterless bound [158]. This establishes un upper-bound for secret key rates when Alice and Bob are connected by a lossy channel with no repeaters. We remark that this bound does not apply to the scenario here presented, where four users are connected to a common server according to some network topology. New bounds were recently found if repeaters are introduced in a chain-like network [159] showing that higher key-rates can in principle be achieved. As our scenario omits repeaters these new bounds do not hold either, however we might expect similar improvements in the maximum key rates as opposed to standard end-to-end 2QKD protocols. Recently, models for fundamental conferencing bounds applying to general networks were introduced [160, 161], although their application to our scenario is not clear.

Our post-processing, is currently based on one-way LDPC error correction. The well-known two-way CASCADE protocol [138] outperforms the optimal LDPC approach in two-party QKD for small QBER [143], however, in the multi-user case this improvement will likely be offset by the additional iterations needed to correct uncorrelated errors in $(N-1)$ raw keys. In contrast, LDPC codes disclose a fixed amount of information that depends only on the largest QBER between Alice and any of the Bobs in the network. To the best of our knowledge, no proof exists for the optimal strategy to achieve the minimal bit disclosure rate when implementing error correction in the multi-user QKD scenario.

A major achievement shown in this chapter was the ability to deliver maximally-entangled multi-partite states through long distances in fibre. The observed key rates were however at least three orders of magnitude lower than those typically achieved in 2QKD. Therefore, experimentally, future steps will be directed towards the engineering of entanglement sources to improve the generation rates of multi-partite entangled states. However, as the exponential decay due to losses in fibres

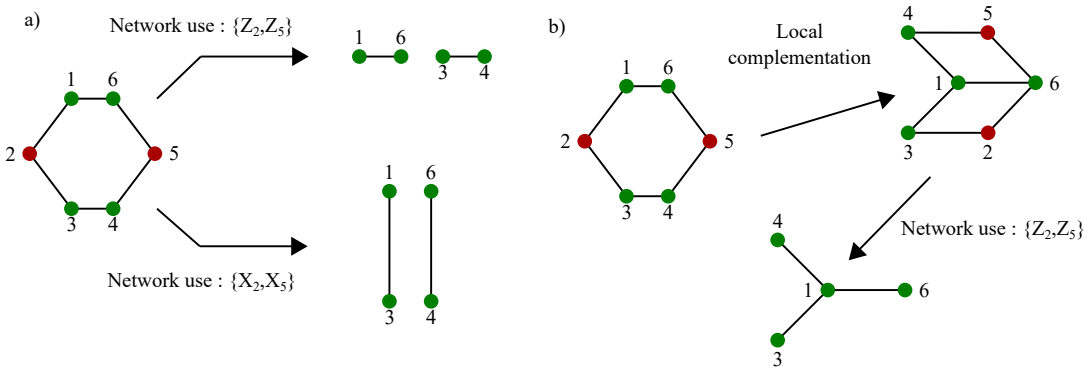


Figure 5.11: **Two CKA approaches in a network scenario.** a) For a 2QKD protocol a local measurement is performed on the red vertices. Following a measurement in the Z-basis pairs 1,6 and 3,4 are left entangled and they establish the keys k_{16} and k_{34} respectively. With another use of the network and X-basis measurements on the red vertices, now pairs 1,3 and 6,4 are left entangled and obtain the keys k_{13} and k_{64} respectively. With an XOR operation the four keys can be mapped into a unique common conference key k_{1346}. b) The N-BB84 protocol is employed to directly obtain k_{1346} with a single network use. The GHZ state required by the protocol is obtained from the starting graph state following local complementation and finally measuring in the Z-basis the red vertices.

scales with the number of parties, direct transmission of multi-partite states will always suffer of a major roadblock compared to the bipartite states employed for 2QKD.

Nevertheless, quantum CKA can outperform 2QKD when N users are arranged within some general network with constrained channel capacity and quantum routers [149, 150, 162–164]. Furthermore, quantum network coding schemes [165] allow the distillation of a shared N-user GHZ state from a single network use, reducing the resource cost—and thus increasing the key rate—achievable in quantum CKA by up to a factor (N-1) [150] when compared with distilling the required number of 2QKD key pairs. We give some intuition on this regard with the help of Fig. 5.11. Suppose that 6 users of a network share the circular graph state (see Sec.2.4) shown in the figure. Starting from this configuration, the "target users" 1,3,4,6 (green vertices) want to obtain a conference key and they can only perform local operations on their qubits or communicate to the "switchboard users" 2,5 (red vertices) to instead perform a local operation on their qubits. If a 2QKD protocol is run as shown in Fig. 5.11a then the target users ask the switchboard users to perform either a measurement in the Z-basis or in the X-basis. Two copies of the initial 6-qubit graph state are required i.e. the network resource is used twice. If instead they prefer a CKA pro-

tocol based on GHZ states they only need local complementation of the starting graph (see Sec. 2.5) and eventually local measurements as shown in Fig. 5.11b. In this case the initial resource is only used once. Therefore in a scenario like the one just sketched the use of CKA protocol based on multi-partite entangled states can increase the key rate of a factor 2. A generalisation and thorough characterisation of the resource cost for N parties, can be a topic for future research.

It is a common belief that quantum network infrastructures will be operative in the near-future, for practical purposes such as the sharing of a secret key between more than two parties. In this chapter, the first experimental demonstration of a conference key agreement protocol was given in a four parties network separated by up to 50 km of telecom fiber, generating shared quantum conference keys of up to 1.15 Mbit. This stands as an alternative to the canonical approach, where pairs of users adopt standard QKD schemes to obtain a set of secret keys turned into a unique conference key with classical operations only. As we learned from the past 30 years of research on QKD, any protocol must take into account the constraints derived from its experimental realisation, and the same holds for conference key protocols. Hence, comparing the two approaches when taking into account experimental constraints is paramount to establish the most convenient protocol, and it is envisioned to be a topic of research for the future.

Chapter 6

Enhanced Multi-Qubit Phase Estimation in Noisy Environments

Quantum technologies are rapidly developing and are expected to outperform their respective classical counterparts in the near future. However, in practice, how near is this future is an open question and technologies such as quantum computers have been recently denominated with the acronym: NISQ, for Noisy Intermediate-Scale Quantum Computing. In fact, the main limitation of these intermediate-scale architectures is the presence of uncorrected noise. In this chapter I present an experimental study aimed to provide an experimentally-friendly approach to the problem of noise in quantum information processing, where the quantum resources are made more robust against noise with the only use of local unitary operations.

I start in Sec. 6.1 with an overview of the concept of noise in quantum theory giving one specific example: the dephasing noise. In Sec. 6.4 the topic of quantum metrology is introduced, its advantages with respect to classical metrology are presented together with its limitations when noise is acting on the system. In Sec. 6.2 the method under study is described and in Sec. 6.3 it will be applied on a 4-qubit system and experimentally demonstrated both on a GHZ state and on a linear cluster state. The entanglement and coherence behaviour of these states will be studied under the effect of the method and a 4-qubit quantum phase estimation protocol will be run in presence of noise successfully showing the efficacy of the local noise protection method proposed. Finally, the results will be discussed in Sec. 6.5.

I note that some of the text in this chapter is excerpted from the research paper

in Ref. [53], where I led the experimental development of the project, from the characterisation and preparation of the full experimental setup to the data acquisition and data analysis.

6.1 Quantum Noise

Noise in quantum mechanics arises from the unavoidable interaction of the system with the environment, and can be formally described with the notion of a *quantum channel*. We consider the joint system-environment as a closed quantum system evolving according to an arbitrary unitary operator U. The state evolves as $U(\rho \otimes \rho_e)U^\dagger$ where ρ and ρ_e are the density matrices of the system and the environment respectively, initially in a separable state. The reduced state of the principal system alone is obtained by tracing out the environment:

$$\mathcal{E}(\rho) = \mathrm{Tr}_e \left[U(\rho \otimes \rho_e)U^\dagger \right]. \tag{6.1}$$

This expression however is not useful in practice, and typically Eq. (6.1) is restated as follows. Suppose $\rho_e = |e_0\rangle\langle e_0|$ is the initial state of the environment expressed in the orthonormal basis $|e_k\rangle$, we can write:

$$\begin{aligned} \mathcal{E}(\rho) &= \sum_k \langle e_k | U\rho \otimes |e_0\rangle\langle e_0| U^\dagger |e_k\rangle = \\ &= \sum_k E_k \rho E_k^\dagger, \end{aligned} \tag{6.2}$$

where $E_k \equiv \langle e_k|U|e_0\rangle$ is an operator acting on the state space of the principal system. Eq. (6.2) is known as the operator-sum representation of $\mathcal{E}$, this formalism is described in detail by Kraus [166], and sometimes E_k is called Kraus operator or operation element of $\mathcal{E}$. The set of operators E_k satisfy the completeness relation

for *trace-preserving* quantum operations, indeed we have:

$$\begin{aligned} 1 &= \mathrm{Tr}\left[\mathcal{E}(\rho)\right] \\ &= \mathrm{Tr}\left[\sum_k E_k \rho E_k^\dagger\right] \\ &= \mathrm{Tr}\left[\sum_k E_k^\dagger E_k \rho\right]. \end{aligned} \tag{6.3}$$

Since this relationship is true for all ρ it follows that we must have

$$\sum_k E_k^\dagger E_k = I. \tag{6.4}$$

Therefore a channel $\mathcal{E}$ transforms in a non-unitary way the density matrix ρ whose trace is preserved. As we shall see in the following, this formalism is very useful to model most of the common non-unitary physical processes labelled in experimental scenarios as noise.

6.1.1 Dephasing noise

As an example of the formalism, we present here possibly the best known quantum channel: the dephasing channel, sometimes called phase damping channel. It describes a non-unitary evolution where only the quantum coherence in the system is affected while preserving the amplitudes. Physically, it describes the random scattering of a photon travelling through a wave guide [167]. In general, after a characteristic time Γ, the off-diagonal elements of the density matrix describing the system decay to zero removing all the coherence present in the state. For these reasons the dephasing channel is often invoked to justify the absence of quantum effects in macroscopic systems, and the quantum-to-classical transition described by decoherence theory [168].

The dephasing channel for a qubit with density matrix ρ is defined as:

$$\mathcal{D}(\rho) = \sum_{k=1}^{2} E_k \rho E_k = (1 - \frac{p}{2})\rho + \frac{p}{2}\sigma_z \rho \sigma_z, \tag{6.5}$$

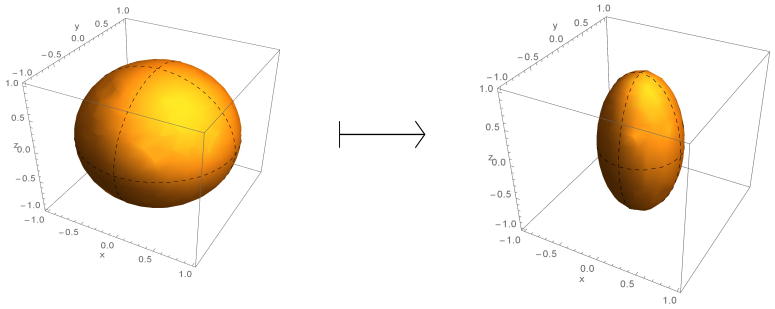


Figure 6.1: Action of the dephasing channel on the Bloch sphere [6], for p=0.5. The input state ρ is shrunk along the $\hat{z}$ axis.

with the Krauss operators

$$E_1 = \frac{\sqrt{p}}{2}(I + \sigma_z) \quad E_2 = \frac{\sqrt{p}}{2}(I - \sigma_z). \tag{6.6}$$

According to Eq (6.5) we apply σ_z to the state with probability $\frac{p}{2}$ and with probability $1 - \frac{p}{2}$ nothing happens. An initial density matrix transforms as:

$$\rho = \begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix} \Longrightarrow \mathcal{D}(\rho) = \begin{pmatrix} \rho_{00} & (1-p)\rho_{01} \\ (1-p)\rho_{10} & \rho_{11} \end{pmatrix}. \tag{6.7}$$

In the limit of $p \to 1$ the off-diagonal terms go to zero. This effect can be more easily physically pictured by considering continuous dephasing. Suppose that the probability of a scattering event per unit time is Γ, so that $p = \Gamma\delta t \ll 1$ when δt is very small. The evolution over a time $t = n\delta t$ is given by $\mathcal{D}^{\otimes n}$ and the off-diagonal terms of the density matrix decay as

$$(1-p)^n = (1 - \Gamma\frac{t}{n})^n \xrightarrow[n\to\infty]{} e^{-\Gamma t}. \tag{6.8}$$

Thus, if we prepare an initial pure state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, after a time $t \gg \Gamma^{-1}$ the density operator decoheres as

$$\begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix} \Longrightarrow \begin{pmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{pmatrix}. \tag{6.9}$$

Using the Bloch representation for the qubit state [6] we can have a characteristic geometric picture of the dephasing channel in Fig 6.1. The effect is of a contraction of the $\hat{x} - \hat{y}$ plane by a factor $(1 - p)$.

6.1.2 Decoherence-Free Subspaces

When considering larger systems decoherence grows exponentially with system size [169]. This represents a major roadblock for quantum computing [167], quantum communication [170] and quantum metrology [171], rendering noise mitigation [172–174] indispensable. Quantum error correction (QEC) [175–177] provides a collection of schemes to in principle achieve full protection against decoherence. To appreciate the achievements of error correction theory and their cost, we briefly present here the topic of decoherence-free subspaces (DFS). DFS is in general the study of subspaces of some Hilbert space where the system is invariant under non-unitary evolution [178], and it was originally developed to specifically avoid decoherence. In the context of error correction, it is a passive error-preventing approach not requiring any active stabilization methods.

Suppose a physical process where a single qubit acquires a phase ϕ if in the state $|1\rangle$, or is left unchanged if in the state $|0\rangle$. In general this transformation is given by the matrix

$$R(\phi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}, \tag{6.10}$$

If the phase ϕ is randomly distributed according to some distribution $p(\phi)$ then the density matrix of the single qubit is the mixed state

$$\int_{-\infty}^{\infty} d\phi \, K(\phi) \rho K^{\dagger}(\phi), \tag{6.11}$$

where $\rho = |\psi\rangle\langle\psi|$ is the initial density matrix of the qubit and $K(\phi) = \sqrt{p(\phi)} R(\phi)$ are the Krauss operators of the non-linear process. It can be shown [179] that if $p(\phi)$ is Gaussian then the expression above leads to decoherence in the qubit. However, if we expand the Hilbert space to two qubits and employ the following encoding

$$|0_L\rangle = |01\rangle \quad |1_L\rangle = |10\rangle \tag{6.12}$$

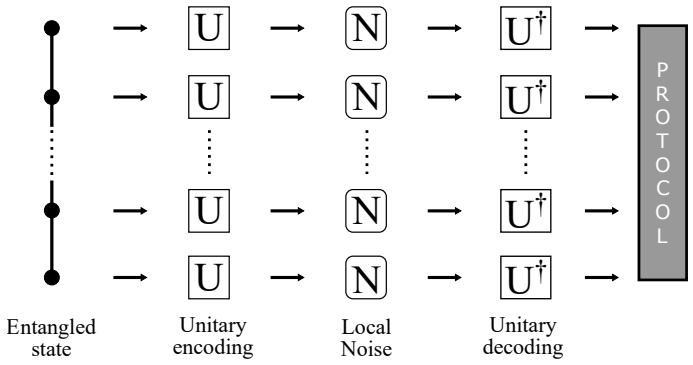


Figure 6.2: **Enhanced noise robustness with local encoding**. An N-qubit entangled state is subject to local dephasing along the z-direction, before it is used for a task such as quantum phase estimation. We use a single-qubit unitary encoding before and after the noise to optimally protect the state's entanglement and coherence, so as to improve its performance in the final metrology task.

where $|0_L\rangle$ and $|1_L\rangle$ are logical qubits encoded by two physical qubits, it is easy to see that the state $|\psi_L\rangle = \alpha|0_L\rangle + \beta|1_L\rangle$ is invariant under dephasing. In other words, the 2-dimensional subspace spanned by $\{|01\rangle, |10\rangle\}$ is decoherence-free. The cost however is the use of two physical qubits to encode a logical qubit.

6.2 Noise Protection by Local Encoding

Error correction can provide full protection against noise, however daunting experimental requirements and large resource overheads [180] make QEC a long-term vision. A complementary approach (see Fig. 6.2), expected to play a central role in near-term quantum technologies, is to relax the fault-tolerance requirement against arbitrary noise aiming instead at enhanced robustness of quantum systems, under experimentally relevant conditions. In this section we present the method introduced in Ref. [181] where noise-robustness is achieved by local encoding of the single qubits before the action of noise. The method was experimentally demonstrated by our group [182], and the experimental results will be presented in this chapter.

We consider here local dephasing $\mathcal{D}(\rho)$ along the Z-axis whose action on quantum states was described in Sec 6.1, and propose simple single-qubit unitary encoding to drastically improve the resilience of quantum resources such as multi-qubit GHZ

states [183]. Consider now, for instance, an N-qubit GHZ state defined as

$$|\mathrm{GHZ}_N\rangle \doteq \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}\right). \tag{6.13}$$

The entanglement of GHZ states affected by independent and identical single-qubit dephasing of strength p is known to decay exponentially with N. More precisely, for the dephased GHZ state $\rho_N(p) \doteq \mathcal{D}^{\otimes N}(|\mathrm{GHZ}_N\rangle\langle\mathrm{GHZ}_N|)$ it holds that $E\left(\rho_N(p)\right) \leq (1-p)^N E\left(\rho_N(0)\right)$ for any convex entanglement quantifier E [184, 185]. However, this scaling can be drastically improved [181] by encoding the state using local Hadamard gates H, defined by $H|0\rangle \doteq |+\rangle$ and $H|1\rangle \doteq |-\rangle$ with $|\pm\rangle \doteq \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. The resulting encoded GHZ state:

$$|\mathrm{GHZ}_N^{\mathrm{enc}}\rangle \doteq H^{\otimes N}|\mathrm{GHZ}_N^{\mathrm{enc}}\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle^{\otimes N} + |-\rangle^{\otimes N}\right), \tag{6.14}$$

has the same entanglement properties, yet its entanglement decay rate becomes independent of N and linear in p. Formally, the dephased encoded state $\rho_N^{enc}(p) \doteq \mathcal{D}^{\otimes N}(|\mathrm{GHZ}_N^{\mathrm{enc}}\rangle\langle\mathrm{GHZ}_N^{\mathrm{enc}}|)$ satisfies the bound $E\left(\rho_N^{enc}(p)\right) \geq E\left(\rho_2(p)\right)$ for all N and thus possesses at least as much resilience as the two-qubit state $|GHZ_2\rangle$, see Ref. [181] for more details. One drawback of the method however is that the optimal encoding depends upon both the state to be protected and the type of noise acting on the system, which therefore should be known in advance. Nevertheless this is not a strong requirement as in practical cases the state to be used in some protocol is typically known and the noise can be estimated with good fidelity. Finally, the method is valid in general for arbitrary graph states and in the following we will focus on the GHZ and linear cluster states for 4 qubits.

6.2.1 Extension to linear cluster graph state

Graph states are a sub-class of multi-qubit states which can be expressed by means of a graph, where vertices represent qubits and links entangling interactions, see Chapter 2 for more details. For $N = 4$ qubits there exist only two classes of connected graph states in-equivalent under local unitary transformation i.e. a state in one class can not be mapped to a state in the other by means of any local unitary operation. The paradigmatic representatives of these two families are the GHZ state

$|\mathrm{GHZ}_4\rangle$ and the linear cluster state $|\mathrm{CL}_4\rangle$, with the latter commonly defined as

$$\begin{aligned}|\mathrm{CL}_4\rangle \doteq & CZ_{1,2}CZ_{2,3}CZ_{3,4}HHHH|0000\rangle = \\ = & \frac{1}{2}(|+00+\rangle + |-10+\rangle + \\ & + |+01-\rangle - |-11-\rangle),\end{aligned} \tag{6.15}$$

where the tensor product is omitted and $CZ_{i,j}$ is a controlled-Z gate [167] on qubits i and j. This expression corresponds to the graph state represented as a linear chain with qubits $1, 4$ as external vertices. By investigating with our protocol both the GHZ and the linear cluster quantum states, we could in essence cover all 4-qubit graph states. The optimal local-unitary encoding for $|\mathrm{CL}_4\rangle$ turns out to be $H \otimes I \otimes I \otimes H$, with I the single-qubit identity operator, resulting in the state

$$|\mathrm{CL}_4^{\mathrm{enc}}\rangle = \frac{1}{2}\left(|0000\rangle + |1100\rangle + |0011\rangle - |1111\rangle\right). \tag{6.16}$$

This state is stabilized by $\{Z_1Z_2, X_1X_2Z_3, Z_2X_3X_4, Z_3Z_4\}$.

6.2.2 Evolution of the purity and entanglement entropy with the environment

Intuitively, one would assume that the noise resilience is achieved by reducing the amount of entanglement with the environment (thus increasing the state's purity). Surprisingly, however, we will show in the following that for the GHZ case, the opposite is true and the encoded states experience a higher loss of purity than the non-encoded ones.

Purity of a density matrix ρ is given by $\mathrm{Tr}\left[\rho^2\right]$ and can be expressed in terms of the eigenvalues λ_k as $\mathcal{P} = \sum_k \lambda_k^2$. The evolved dephased unencoded GHZ state has eigenvalues

$$\lambda_0 = (1/2)(1 - (1-p)^N), \tag{6.17}$$

$$\lambda_1 = 1 - \lambda_0, \tag{6.18}$$

leading to $P(\rho^N(p)) = \frac{1}{2}\left(1 + (1-p)^{2N}\right)$. On the other hand, the encoded state has eigenvalues given by

$$\lambda_k = (1-p/2)^{N-k}(p/2)^k + (1-p/2)^k(p/2)^{N-k}, \tag{6.19}$$

with $0 \leq k \leq N-1$ (each with a degeneracy of $\binom{N-1}{k}$) leading to a purity $P(\rho_T^N(p)) = \left(p^N(1-\frac{p}{2})^N + (1-p+\frac{p^2}{2})^N\right)$. Although both purities decay exponentially with N, the purity of the unencoded are state tends to $1/2$, while the purity of encoded state tends to 2^{1-N}.

The entanglement between system and environment can also be quantified via the von Neumann entropy of the system

$$S(\rho) = \mathrm{Tr}(\rho \log_2 \rho) = -\sum_k \lambda_k \log_2 \lambda_k. \tag{6.20}$$

For this quantity, closed formula expressions are not no longer possible but one can easily see some interesting properties. For the unencoded GHZ state the entanglement entropy tends to $S(\rho_N(p)) = 1$ while for the encoded state $S(\rho_N^T(p)) = N-1$ as $p \to 1$. Moreover, for any $p > 0$ it follows that $S(\rho_N^T(p)) > S(\rho_N(p))$, that is, at all times of the noisy evolution the encoded and more robust state is surprisingly more entangled with the environment.

Intuitively, this can be understood as a consequence of the special structure of the GHZ state, which even after full dephasing retains classical correlations that manifest in relatively high residual purity. In the encoded case, the coherence is more distributed, thereby reducing the resilience of the state's purity. In the case of the linear cluster, on the other hand, the unencoded state features uniformly distributed populations, while the encoded state is sparser. As a consequence, the optimal encoding protects both entanglement *and* purity.

6.3 Experimental Results

In the previous section we described the method proposed in Ref. [181] where GHZ and Linear cluster states' robustness against dephasing noise is enhanced by local encoding single qubits before the action of the noise. In this section, the method

is experimentally tested on a photonic platform albeit in general, it is worth noting that the method could be applied to any other experimental architecture commonly dealing with dephasing noise, from spin qubits to trapped ions, without any increase in experimental complexity. The details of the experimental setup have been extensively described Chapter 3 and in Fig. 6.3 only a scheme of the setup employed to generate both the GHZ states and linear cluster states is shown.

Qubits are encoded in the horizontal $|h\rangle \equiv |0\rangle$ and vertical $|v\rangle \equiv |1\rangle$ polarization states of single photons. These are generated at 1550 nm via collinear type-II spontaneous parametric down-conversion in a 22 mm long PPKTP crystal, pumped with a 1.6 ps pulsed laser at 775 nm. After spectral filtering with a bandwidth of 3 nm, the source generates ~ 3075 pairs/mW/s with a symmetric heralding efficiency of $\sim 55\%$. Embedding the crystal within a Sagnac interferometer [46] enables the generation of high-quality entangled states of the form

$$|\psi^-\rangle = \frac{1}{\sqrt{2}} \left(|h\rangle|v\rangle - |v\rangle|h\rangle\right), \tag{6.21}$$

with typical fidelities $F(\rho_e, \rho_t) = (Tr[\sqrt{\sqrt{\rho_t}\rho_e\sqrt{\rho_t}}])^2 = 99.62^{+0.01}_{-0.04}\%$ where ρ_e and ρ_t are the experimental and target state respectively. The measured purity is $P = 99.34^{+0.01}_{-0.09}\%$ and entanglement as measured by the concurrence [22] is $\mathcal{C} = 99.38^{+0.02}_{-0.10}\%$. Using two such photon-pair sources in the setup of Fig. 6.3, we can prepare the 4-qubit GHZ state $|\mathrm{GHZ}_4\rangle$ of Eq. (6.13) by subjecting one photon of each entangled pair to nonclassical interference on a polarizing beam splitter (PBS), which transmits horizontal and reflects vertically polarized photons. This implements the type-I fusion gate [47] (see Sec 3.6) for which we achieved a visibility of $91.80^{+1.73}_{-1.73}\%$, translating into a purity of $P = 87.09^{+1.15}_{-2.18\%}$ and fidelity of $F = 92.53^{+0.63}_{-1.23}\%$ for the 4-qubit GHZ state. The states are generated at a measured rate of 47.6 Hz using 60 mW pump power. The linear cluster $|\mathrm{CL}_4^{\mathrm{enc}}\rangle$, on the other hand, is generated by subjecting one photon of an entangled pair to two sequential fusion gates with uncorrelated single photons in the state $|+\rangle$ and with a Hadamard gate in between. This results in slightly lower purity of $\mathcal{P} = 81.77^{+0.65}_{-0.85\%}$ and fidelity of $F = 89.03^{+0.38}_{-0.60}\%$.

Single qubit dephasing of Eq. (6.5) is experimentally implemented in a controllable manner by applying the identity channel for a time $1 - p/2$ and the σ_z channel for a time $p/2$. For simplicity, these operations together with encoding and decoding,

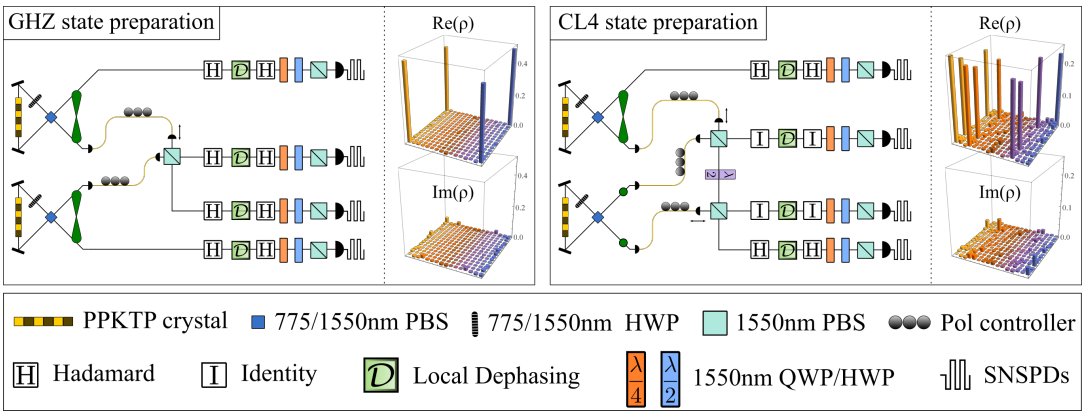


Figure 6.3: **Preparation of 4-qubit GHZ (left) and linear cluster (right) states and encoding stage**. The encoding in both cases corresponds to single-qubit Hadamard (H) gates or identity (I) operations. The state is then locally encoded, dephased, decoded, and measured using a combination of quarter-waveplate (QWP), half-waveplate (HWP), PBS, and superconducting nanowire single photon detectors (SNSPDs) with four-fold coincidence detection. On the right, the real and imaginary part of the experimental density matrices (without dephasing) are shown. For the GHZ is the unencoded state whereas for the linear cluster is the encoded state.

are applied as appropriate rotations of the measurement frame. The density matrices of the experimentally generated states are then reconstructed using maximum-likelihood quantum state tomography. The tomography was performed using the set of symmetric informationally complete (SIC) measurements [186], which reduces the number of measurements compared to the standard Pauli basis by a factor $(2/3)^N$, leading to improved precision at equal acquisition time.

6.3.1 Negativity and Purity enhancement

We start by investigating the behaviour of one of the most paradigmatic quantum resources: quantum entanglement, as measured by the negativity in the partition $(1 \mid 234)$, see Sec. 2.6 for the definition.

Figure 6.4 shows that the negativity of the encoded $|\mathrm{GHZ}_4^{\mathrm{enc}}\rangle$ and $|\mathrm{CL}_4^{\mathrm{enc}}\rangle$ states is significantly more resilient against dephasing than the unencoded states. In the case of the linear cluster, it is even possible to qualitatively change the behavior from finite-time disentanglement to infinite-time disentanglement. Moreover, the inset in Fig. 6.4 confirms in the case of GHZ states (note that for $N < 4$ the linear cluster and the GHZ are equivalent), that the enhancement for a fixed amount of dephasing becomes more significant as the number of qubits increases, instead of

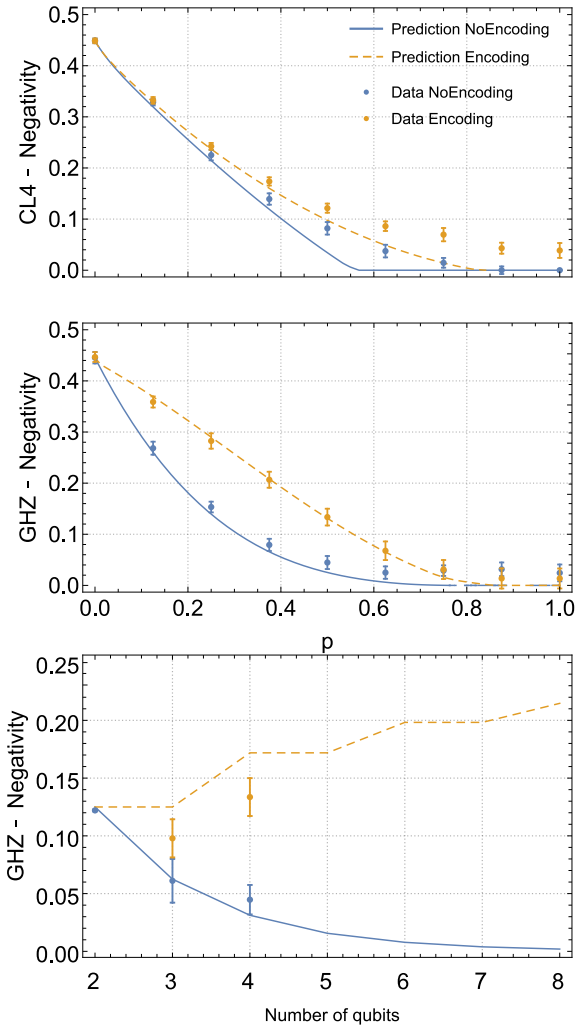


Figure 6.4: **Resilience enhancement of the negativity in the partition** $(1|234)$**.** Shown is the negativity of the GHZ (left) and linear cluster (right) with (dashed-orange) and without (solid-blue) encoding. The solid (dashed) lines depict the theoretical predictions with the experimental unencoded (encoded) input state. In the top-right inset the trend of the GHZ negativty is shown in terms of the number of qubits and at fixed noise $p = 0.5$. With the encoding proposed, the entanglement is best protected when the number of qubits increases. Error bars represent 3σ statistical confidence regions obtained from a Monte-Carlo routine taking into account the Poissonian counting statistics.

the exponential decay observed for the unencoded states [181]. For both the GHZ state and linear cluster, we consider all the 1-vs-rest partitions $(i|jkl)$ and 2-vs-2 bipartitions : $(12|34), (13|24), (14|23)$. The transversal 4-GHZ state is optimally protected in all the 1-vs-rest and 2-vs-2 partitions. The scenario is more complex when instead we study the linear cluster, in fact there always exists at least one 1-vs-rest partition where the protection is optimal. However, the partition depends from the encoding chosen.

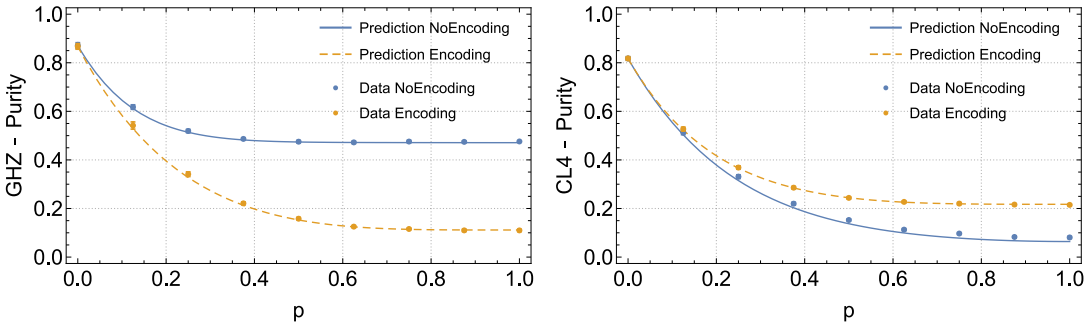


Figure 6.5: **Experimental results for the purity under local encoding**. Shown is the purity of the GHZ (left) and linear cluster (right) states with (dashed-orange) and without (solid-blue) encoding. The solid (dashed) lines depict the theoretical predictions with the experimental unencoded (encoded) input state. Interestingly, conversely to the GHZ case, the purity of the linear cluster is enhanced by the local encoding. The 3σ error bars, obtained as previously, are smaller than the symbol size.

6.3.2 Robustness of Coherence

The coherent superposition of states is a remarkable feature of quantum mechanics. Quantum coherence has therefore a fundamental importance and it was recently rigorously formalised as a physical resource [187] with its own characterization, quantification, manipulation, dynamical evolution, and operational application. In this section we study the dynamics of coherence of locally encoded states under decoherence. We use the recently developed resource theory of multilevel coherence [188, 189] to quantify through the *robustness of multilevel coherence* the decay of coherence under dephasing noise, see Ref. [189] for more details on this coherence measure. We consider composite N-qubit systems and measure coherence with respect to the computational basis $\{|0\rangle, |1\rangle\}^{\otimes N}$. In order to capture the structure of coherence in such a system, one first defines the following sets of states

$$\mathcal{C}_k := \mathrm{conv}\{|\psi\rangle\langle\psi| : r_{\mathrm{C}}(|\psi\rangle) \leq k\}, \tag{6.22}$$

where conv stands for convex hull[1] and r_{C} is the coherence rank of $|\psi\rangle$, given by the number of non-zero coefficients in the basis-decomposition of $|\psi\rangle$. $\mathcal{C}_1$ is the set of fully incoherent states, given by density matrices that are diagonal in the computational basis, while $\mathcal{C}_d \equiv \mathscr{D}(\mathscr{H})$ is the set of all states in the d-dimensional

[1]The convex hull of a set of points is defined as the smallest convex polygon, that encloses all of the points in the set.

Hilbert space $\mathscr{H}$. It was shown in Ref. [189] that these sets obey a strict hierarchy and that the amount of k-level coherence can be quantified by the robustness of multilevel coherence

$$R_{\mathcal{C}_k}(\rho) := \inf_{\tau \in \mathscr{D}(\mathscr{H})} \left\{ s \geq 0 : \frac{\rho + s\tau}{1+s} \in \mathcal{C}_k \right\}. \tag{6.23}$$

Here τ is any density matrix. Eq. (6.23) can be seen as a quantifier of the minimal mixing required to make the state incoherent. A state has coherence number k, if it can be decomposed into pure states which are superpositions of at most k basis elements, while every decomposition must contain at least one such state. For $k = 1$, this measure simply quantifies the total amount of coherence in the system [188]. Experimentally, we can quantify the multilevel coherence for a given density matrix using a semi-definite program as specified in Ref. [189]. Multi-level coherence is independent of entanglement measures, therefore unlocks information on the encoding effects otherwise inaccessible. This, as we will see in the next section, provides useful insights on phase estimation in noisy environment.

Intriguingly, the left panel in Fig. 6.6 shows that the encoded GHZ_4 states maintain a constant amount of coherence for arbitrary dephasing, while the unencoded states show an exponential decay. Intuitively, this may again be understood based on the distribution of coherence within the state. Concentrating all coherence on two terms (coherence rank 2), such as the unencoded GHZ_4 state leaves the state vulnerable to dephasing, as opposed to maximally spreading it out (coherence rank 2^N), such as the encoded state, achieving increased resilience. In the latter case indeed, the decoding map (a non-free operation in the resource theory of coherence) can under certain conditions recover a significant amount of coherence. This effected was also called coherence "freezing" and it was studied experimentally under bit-flip noise in a related work, see [190].

On the other hand, for the linear cluster in the right panel of Fig. 6.6, constant behavior cannot be achieved, due to subtle differences in the structure of the states. Nonetheless protection is observed for all the values of dephasing. This behavior is confirmed at all coherence levels, and for $k = 2$ and $k = 3$ the results are shown in the inset of the right panel in Fig. 6.6.

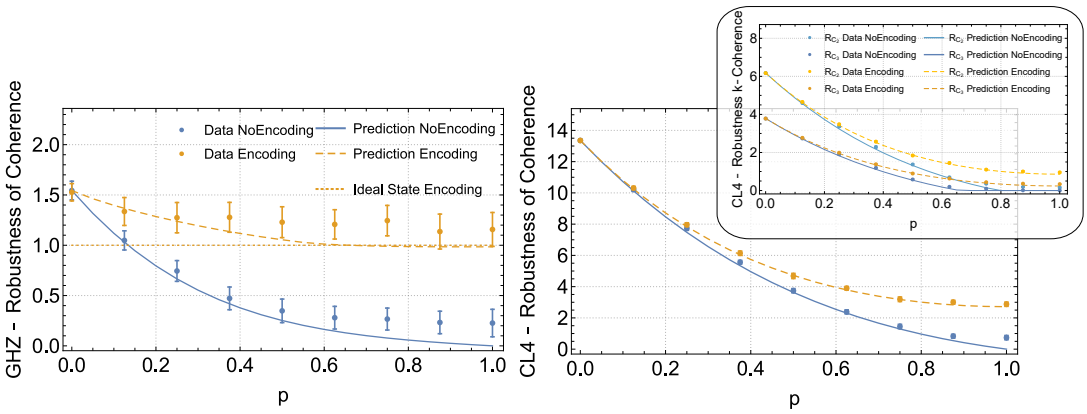


Figure 6.6: **Resilience of coherence against dephasing noise.** Robustness of coherence R_{C_1} for the 4-qubit GHZ (left) and linear cluster state (right). The solid-blue lines represent the theory prediction when the states are not encoded, compared with the encoded scenario given by the dashed-orange lines. For the GHZ state only, the theory prediction starting with an ideal input encoded state is shown with a dotted-orange curve. Note that experimental imperfections tend to lead to additional coherence terms compared to the ideal GHZ state. The robustness of coherence reflects this as higher initial values of coherence and non-vanishing coherence for all dephasing strengths. Experimental data is shown as blue (orange) dots for the non-encoded (encoded) case with 3σ error bars smaller than the symbol size. In the inset, shown is the robustness of 3-level (R_{C_2}) and 4-level (R_{C_3}) coherence the unencoded (blue) and encoded (orange) linear cluster. The encoding provides enhanced protection of coherence at all levels and for all values of p.

6.4 Quantum Metrology

We have seen so far how simple local encoding can provide robustness against noise. We attested the efficacy of the approach respect to fundamental physical quantities such as entanglement, purity and coherence. In this section, we test the protocol in practice in a quantum metrology task in presence of noisy environments.

Quantum metrology [191] is a fruitful area of study within quantum information theory [192] providing strategies to estimate an unknown parameter θ with a given resource. Let assume that we want to estimate θ by measuring a quantity M on a given system. The distribution of the possible values x of M given a value of θ can be in general described by a probability density function $f(x;\theta)$. As our task is to estimate θ indirectly from the observed values x, we can build an estimator $\hat{\theta}(x)$ giving the value of the unknown parameter θ from a value of x. Although in general it is not possible to obtain the "true value" of θ it is possible to compute the lower

bound for the variance of the estimator

$$\mathrm{Var}[\hat{\theta}(x)] = \langle \hat{\theta}^2(x) \rangle - \langle \hat{\theta}(x) \rangle^2 \geq \frac{1}{\mathcal{F}(\theta)}, \tag{6.24}$$

where $\mathcal{F}(\theta)$ is the Fisher information, a mathematical tool very useful in information theory either classical [193] or quantum [194] and defined as

$$\mathcal{F}(\theta) = \int dx\, f(x;\theta) \left(\frac{\partial}{\partial \theta} \log f(x;\theta) \right)^2. \tag{6.25}$$

The lower bound in Eq. (6.24) is also known the Cramer-Rao bound [195, 196] valid for estimation of unbiased parameters i.e. such that the estimator satisfies

$$0 = \int dx\, (\theta - \hat{\theta}(x)) f(x;\theta), \tag{6.26}$$

that is, the expectation value of the estimator is equal to θ. We can extend these arguments to the realm of quantum information, by invoking the Born rule and defining the probability density function of a projective measurement $|x\rangle\langle x|$ corresponding to the outcome x on a quantum states ρ_θ as

$$f(x;\theta) = \mathrm{Tr}\left[\rho_\theta |x\rangle\langle x|\right], \tag{6.27}$$

leading to the *quantum* Cramer-Rao bound [194, 197]

$$\mathrm{Var}[\hat{\theta}(x)] \geq \frac{1}{\mathcal{F}_Q(\theta)}, \tag{6.28}$$

where $\mathcal{F}_Q(\theta)$ is the *quantum* Fisher information [194, 197]. In particular, if the parameter θ is a phase imparted to the state by a unitary evolution $U_\theta = e^{-i\theta H}$ described by the Hermitian operator H, the quantum Fisher information can be expressed with a closed formula [194, 197]

$$\mathcal{F}_Q[\rho_\theta, H] = 2 \sum_{i,j} \frac{(p_i - p_j)^2}{p_i + p_j} |\langle i|H|j\rangle|^2, \tag{6.29}$$

where the p_i are the eigenvalues of ρ_θ relative to the eigenstates $|i\rangle$. As an example, if we assume $H = \frac{\sigma_z}{2}$ then it can be shown [192] that for N-qubit separable states

$\mathcal{F}(\rho_\theta) \leq N$, namely the QFI is bounded by the shot-noise limit (SNL), while for GHZ states the QFI attains the optimal value $\mathcal{F}_{\max} = N^2$, known as the Heisenberg limit.

6.4.1 Enhanced phase estimation

We now exploit our passive error correction for quantum metrology, by performing a 4-qubit phase estimation task [192] in a noisy environment. The goal is to estimate an unknown phase ϕ imparted on a probe state ρ by the unitary $U_\phi = e^{-\frac{i}{2}\phi\sigma_z}$ by appropriately measuring the evolved state $\rho_\phi \doteq U_\phi^{\otimes N} \rho U_\phi^{\dagger \otimes N}$. It is well known that GHZ states with local measurements in the Pauli-X basis are optimal for phase estimation [171]. In the presence of dephasing noise, however, this task becomes much more challenging, and different inequivalent strategies can be devised [198, 199]. We now show how our local encoding can significantly enhance the metrology performance of 4-qubit GHZ state under such conditions. To assess the performance of phase estimation we study the expectation value:

$$\mathrm{Tr}\left[\rho_\phi \left(|+\rangle\langle+|\right)^{\otimes 4}\right]_{\mathrm{GHZ}} = \frac{1}{16}\left((p-1)^4\cos(4\phi)+1\right),$$

for noise of strength p, showing that for maximal dephasing, $p \to 1$, no phase information can be recovered. Conversely, if the local encoding of Eq. (6.14) is used the expectation value takes the more complex form

$$\begin{aligned}\mathrm{Tr}\left[\rho_\phi \left(|+\rangle\langle+|\right)^{\otimes 4}\right]_{\mathrm{GHZ}^{enc}} =& \frac{1}{128}(-4p^4\cos(2\phi) + p^4\cos(4\phi) + \\ & 3p^4 + 16p^3\cos(2\phi) - 4p^3\cos(4\phi) - \\ & 12p^3 - 24p^2\cos(2\phi) + 12p^2\cos(4\phi) + \\ & 12p^2 + 16p\cos(2\phi) - 16p\cos(4\phi) + \\ & 8\cos(4\phi) + 8),\end{aligned} \tag{6.30}$$

which for full dephasing ($p = 1$) preserves phase sensitivity:

$$\mathrm{Tr}\left[\rho_\phi \left(|+\rangle\langle+|\right)^{\otimes 4}\right]_{\mathrm{GHZ}^{enc}} = \frac{1}{128}(4\cos(2\phi) + \cos(4\phi) + 11).$$

Although entanglement is recognized as a fundamental resource for phase estimation [200, 201], is is remarkable to note that phase sensitivity is observed even in the full dephasing regime, whereby the entanglement is always zero, even for the encoded states. It follows that the phase sensitivity observed is instead provided by the coherence only, which as we have previously seen is left untouched by the dephasing. Only when both coherence and entanglement are zero (as for the non-encoded states) the phase sensitivity is completely suppressed. This suggests, at least for this specific scenario, coherence is the useful resource whereby the entanglement is not.

Experimentally, we applied a phase-shift $\phi \in [0, \pi]$ to each qubit, by rotating the measurement frame accordingly, and reconstructed the expectation values $\mathrm{Tr}\left[\rho_\phi \left(|+\rangle\langle+|\right)^{\otimes 4}\right]$ as a function of ϕ for a range of p, see Fig. 6.7a. The results clearly show a steeper slope of $\mathrm{Tr}\left[\rho_\phi \left(|+\rangle\langle+|\right)^{\otimes 4}\right]$ for the encoded state compared to the unencoded state for all non-zero values of ϕ. This directly translates into a more sensitive phase estimator in the encoded case. Moreover, we emphasize that the encoded fringes preserve at least half the visibility of the $p = 0$ case, even for $p = 1$ where instead, without our encoding, the unencoded fringes flatten to a constant value. In other words, whereby phase estimation would be normally impossible, our encoding makes it feasible again.

This qualitative behavior is turned into a quantitative result by measuring the experimental variance of the estimated phase at the point where the fringes are the steepest for different values of p, according to

$$\mathrm{Var}[\phi] = \frac{\mathrm{Var}[\epsilon]}{|\frac{d}{d\phi}\epsilon|^2}, \tag{6.31}$$

where ϵ is the measured average value of our estimator $\epsilon \equiv \langle +_1 +_2 +_3 +_4 \rangle$. The results are shown in Fig. 6.7b.

Finally, we study the effects of encoding using the quantum Fisher information introduced in Sec. 6.4. When the estimation is obtained by ν repetition runs,

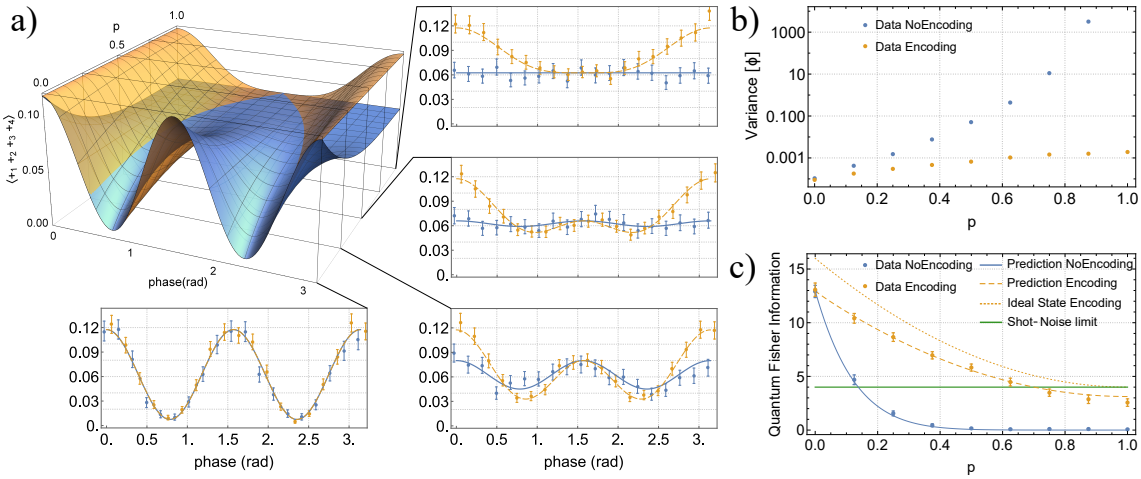


Figure 6.7: **Phase estimation with and without encoding.** **a)** Expectation value $\langle +_1 +_2 +_3 +_4 \rangle$ as a function of phase and amount of noise p, for a locally encoded (orange) and a non-encoded (blue) 4-qubit GHZ state. In particular, for values of $p = 0, 0.25, 0.5, 1$ the experimentally measured expectation values as a function of the phase are shown. The theoretical predictions are shown as blue-solid (no encoding) and orange-dashed (encoding) curves, and error bars indicate 3σ statistical uncertainty regions obtained from a Monte Carlo resampling of our Poisson counting statistics. In the absence of noise ($p = 0$) there is no difference between encoded and unencoded states. With increasing dephasing, however, the advantage of the encoding becomes clear in that the expectation values for unencoded states decay to zero, but remain non-zero for all p if the local encoding is used. **b)** Robustness enhancement of the quantum Fisher information. QFI of the encoded (dashed-orange) and non-encoded (solid-blue) states, compared with the shot-noise limit (solid green). Without encoding, the GHZ state loses its advantage already in the low-noise regime. In contrast, as shown in the figure, the encoding preserves the QFI for all values of dephasing, ideally (dotted-orange), and up to $p = 0.6$ experimentally. **c)** Comparison of the phase variance without (blue) and with (orange) encoding, for different noise strengths. Notably, with encoding, the variance observed is up to 2 orders of magnitude smaller than the case without, where the error on the inferred phase diverges with increasing noise.

the statistical deviation $\mathrm{Var}[\phi]$ in the estimation of ϕ, is bounded as $\mathrm{Var}[\phi] \geq 1/\nu\mathcal{F}(\rho_\phi)$ [202]. For GHZ states and in the noiseless case, we have $\mathcal{F}_{\max} = N^2$ whereas the QFI of a locally dephased GHZ state is $\mathcal{F}(\rho_N(p)) = N^2(1-p)^{2N}$ indicating that for fixed noise strength p the precision of the estimate of ϕ decreases exponentially with N. Notably, such drastic decay is turned into a quadratic one for the encoded GHZ state, $\mathcal{F}(\rho_N^{\mathrm{enc}}(p)) = N^2(1-p)^2 + 4N\big(1-\frac{p}{2}\big)\frac{p}{2}$. The Fisher information is measured experimentally for both the encoded and non-encoded density matrices [203], see Fig. 6.7c. In absence of noise, we experimentally observe a value close to the Heisenberg limit $N^2 = 16$, which exponentially drops to 0 with

increasing noise when no encoding is applied. Encoded GHZ states, on the other hand, preserve their quantum advantage for significantly high noise strengths. Here, we have considered that the noise acts before the phase is imprinted on the system. However, the same robust behaviour would also be observed in either the case where the noise and the phase evolution happen simultaneously [204], or when the noise happens after the phase is imprinted, thus showing the wide applicability of our approach.

This can be shown explicitly accounting for the time evolution. We consider a frequency estimation task where the probe states evolve according to the Hamiltonian $\mathcal{H} = \frac{\omega}{2}\sum_{k=1}^{4}\sigma_z^k$ with ω the frequency to be estimated. Following the treatment in Ref. [204], the noisy evolution is described by a master equation of the Lindblad form

$$\frac{\partial\rho(t)}{\partial t} = \mathcal{H}(\rho) + \mathcal{L}(\rho). \tag{6.32}$$

Here, $\mathcal{H}(\rho) = -i[H,\rho]$ and the Liouvillian $\mathcal{L}(\rho)$ simplifies to $\sum_k \mathcal{L}^k$ for uncorrelated noise. We now consider two cases: dephasing acting in the same direction of the phase rotation given by

$$\mathcal{L}^k\rho = -\frac{\gamma}{2}[\rho - \sigma_z^k\rho\sigma_z^k], \tag{6.33}$$

and dephasing transversal to the Hamiltonian $\mathcal{H}$ given by

$$\mathcal{L}^k\rho = -\frac{\gamma}{2}[\rho - \sigma_x^k\rho\sigma_x^k]. \tag{6.34}$$

Here, γ is the noise strength. As shown in Appendix A of Ref. [204] solving the master equation Eq. (6.32) leads to a single-qubit map expressed in terms of Kraus operators of the form

$$\mathcal{E}_\omega(\rho) = \frac{1}{2}\sum_{i,j} S_{i,j}\sigma_i\rho\sigma_j. \tag{6.35}$$

All elements of the S matrix are zero except $S_{00} = a+b, S_{11} = d+f, S_{22} = d-f, S_{33} = a-b, S_{03} = ic, S_{30} = -ic$ with a, b, c, d and f real coefficients depending on ω, γ, and t. In the case of parallel noise (corresponding to our no-encoding scenario) we

get

$$a = 1,$$

$$b = e^{-t\gamma} \cos t\omega,$$

$$c = e^{-t\gamma} \sin t\omega,$$

$$d = f = 0,$$

whereas in the case of transversal-dephasing (corresponding to our enconding scenario) we obtain

$$a = 0,$$

$$b = e^{-t\gamma} \cos t\omega,$$

$$c = e^{-t\gamma} \sin t\omega,$$

$$d = f = 1.$$

It can be shown that, with a GHZ input state, only the latter case of transversal-dephasing leads to a superclassical precision scaling of $\propto 1/N^{5/6}$ thus proving the efficacy of our method even in this scenario.

We consider now for completeness the last scenario i.e. the noise acting on the state after the phase is imprinted. This could be the case, for example, of a scenario where the state after the phase rotation is stored in a memory for some time before the measurement stage. Although the practicality of such a scenario might be unclear at the moment, we speculate whether it might result useful in some network-based protocol, where different nodes require synchronization. Either way, we observe that if the state is encoded, dephased and then decoded after the phase is imprinted, the expectation value of the estimator is

$$\langle +_1 +_2 +_3 +_4 \rangle = \frac{1}{8}(\cos 2\phi)^2, \tag{6.36}$$

namely, it does not depend on the dephasing strenght p. Therefore, we conclude that the single-qubit encoding and decoding result it is useful even in this scenario.

6.5 Discussion and Conclusions

With the local encoding approach we suggested in this chapter full error correction is not possible, therefore it can not replace the already well established theory of error correction based on the use of many physical qubits to encode one logical qubit, which however will be only possible in the long-term. We emphasize that one of the most notable strengths of our method is that it *does not* require particular technological innovation. While the experiment was performed in a multiqubit photonic platform, the approach can be incorporated into virtually any current quantum experiment based on any quantum technology. In particular, the applicability extends to any scenario and experimental platform where the noise has a preferred direction, such as dephasing typically seen in systems like spin qubits or trapped ions. These features make the proposed approach highly practical in a wide range of current quantum devices.

Phase estimation with sensitivity going beyond the classical limit was demonstrated in presence of noise. The experimental results shown are obtained in a scenario where the noise acts before the phase estimation protocol, which is relevant in scenarios where the quantum system is subject to a noisy environment before being used for a protocol that operates on a much faster timescale, such that decoherence during the protocol can be neglected. Furthermore it could be extremely helpful, in any controlled experimental environment where noise cannot be assumed to act *only* during the protocol, but rather during the often lengthy state preparation steps. Moreover, beside the phase estimation scenario, one could think of quantum communication / QKD protocols, or situations where a quantum system has to idle in a dephasing environment (e.g. a quantum cache memory) before it can be used. Hence, the experiment here presented should be thought of as a comprehensive study of the benefits of local encoding, where the instance of noisy phase estimation can be seen as a proof-of-principle whose results hold, qualitatively, even in the case of simultaneous noise and quantum information task.

Finally, on a more fundamental character, we revealed counter-intuitive behaviour where encoded GHZ-states manifest lower purity (higher entanglement with the same environment we are protecting the states from) while nonetheless showing robustness from dephasing noise compared to those without encoding. Even more, for GHZ-states, independence of coherence from dephasing noise was observed without requiring resource-costfull error correction protocols.

We envision our method to be particularly relevant for protecting multi-qubit graph states from noise during distribution over quantum networks, before being used in measurement-based quantum computing, or when stored in quantum memories. Moreover, the enhanced robustness of the encoded states under dephasing noise can lead to exponentially larger violation of multipartite Bell inequalities [181]. Such a violation could then be used, for instance, in multipartite device-independent cryptography protocols, randomness certification, or to achieve a reduction in the amount of communication required to compute a function in a distributed manner.

In conclusion, we successfully demonstrated an alternative route for noise-protection which might be further exploited as long as active multi-qubit quantum error correction remains out of reach for near-term technology.

Chapter 7

Conclusions

When I started writing this thesis I complained I did not have one single story to tell, but rather three independent ones. Like during my Ph.D., we jumped from an experiment where observers are observed and our natural notion of objective facts is not that clear anymore, to experiments where the challenge was to send graph states through long fibres or to perform information processing in noisy environments. Now, at the end of this journey, I acknowledge that I was wrong to complain. With the experiment presented in Chapter 4, I questioned what is an observation, what qualifies as an observer and why in quantum mechanics observers and observations have a special role in first place. I showed that with a minimal definition, even a single photon can be an observer, and that if we believe in a local nature with free choices, then "facts of the world" must be only relative to the observer who established them.

Diving into the foundations of quantum mechanics can be fascinating but we should not forget that after all, this thesis was written by an experimentalist. In this regard, we found more practical challenges in Chapter 5 and Chapter 6. In Chapter 5, I experimentally demonstrated for the first time how multi-photon graph states can be used to achieve technical goals such as the sharing of a secret conference key between several parties. A remarkable result shown in Chapter 5 was the ability to send multi-photon graph states to distances up to 50 km, while preserving their quality. I hope the experiment shown in Chapter 5 can be a primer for future experimental protocols based on multi-photon states.

Finally, in Chapter 6, I approached a very hot topic for present quantum tech-

nologies, that is how to account for noise when implementing any protocol in practice. This problem is particularly relevant for the modern race to the realisation of a quantum computer. The method demonstrated in Chapter 6 diverts from the route towards the full error correction, preferring instead the use of local encoding of a given quantum resource state, unlocking passive robustness with respect to a given type of noise. This is certainly not a general solution, but it definitely provides an approach experimentally feasible with current technology.

All the experiments shown in this thesis were realised with the same setup: a photonic platform. Photonics and quantum information processing have been a very good match for decades. In particular, probabilistic single-photon sources, as those presented in this thesis, have been extensively used for countless of experiments. Will this hegemony persist in the next decades? I believe it will. Quantum information technologies can be divided in three big groups: quantum computing, quantum communication and quantum sensing. The photonic platform used in this thesis was build on a 3x1.5 meters optical bench, it can produce up to one 6-photon graph state every second and can only generate a limited number of quantum states. Therefore, it is unlikely to be used as a quantum computer in the future. But the same is not true for silicon photonic qubits produced by four-wave mixing, whose compatibility with the well-established semiconductor facilities, recently attracted important investments and it might surpass the current two main candidates (superconducting and trapped ion platforms) to the realisation of a quantum computer.

Quantum communication and quantum sensing will instead definitely be the domain of photonics, at least where distribution of qubits is demanded. Whether the photons will be generated from PDC or from other sources as for example quantum dots, is not easy to envision. Either way, I believe that the state-of-the-art technology will remain mostly steady as long as fast and low-loss optical switches will not be available. When they will, an array of probabilistic PDC sources will encode one nearly-deterministic source. A high-rate deterministic source of graph states might then be a reality.

Appendix A

Independent high-purity photons created in domain-engineered crystals

In this Appendix I include our experimental paper [205] based on the theoretical work in Ref. [37]. This work is strictly related to the problem of spectral correlations between single photons generated by a PDC process, as presented in Sec. 3.2. In fact, when two single photons generated in two independent sources interfere, as for example in a fusion gate (see Sec 3.6), the quality of the interference effect [206] is drastically degraded when the two photons are not perfectly indistinguishable in all the degrees of freedom (DOF). In the experiment here reported we focus on the spectral DOF, which is controlled with novel domain-engineering techniques. We compared the quality of the independent interference with the standard PPKTP crystals and our engineered crystals. We showed that our crystals outperform the PPKTP ones, when no narrow-band filtering is employed, whereas are comparable with PPKTP crystals when spectral filtering is employed. However, as the spectral reduces the heralding efficiency and brightness of the source (see Sec 3.3), our crystals should be preferred when taking into account also these parameters.

In the following the research paper resulted from the experiment is included. I contributed with the optimisation of the sources employed in the experiment, by studying the heralding efficiency and brightness as a function of the pump size (see Fig 3.5 in Sec. 3.3). I contributed in part of the data collection and data analysis.

Letter Vol. 5, No. 5 / May 2018 / Optica 514

Independent high-purity photons created in domain-engineered crystals

Francesco Graffitti,* Peter Barrow, Massimiliano Proietti, Dmytro Kundys, and Alessandro Fedrizzi

Scottish Universities Physics Alliance (SUPA), Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, UK
**Corresponding author: fraccalo@gmail.com*

Received 22 December 2017; revised 23 March 2018; accepted 4 April 2018 (Doc. ID 318273); published 30 April 2018

Advanced photonic quantum technology relies on multi-photon interference, which requires bright sources of high-purity photons. Single-photon sources based on nonlinear parametric processes typically require lossy spectral filtering for enhancing the spectral purity of the heralded photons. Here, we implement a novel domain-engineering technique for tailoring the nonlinearity of a parametric down-conversion crystal in order to generate indistinguishable and spectrally pure photons without filtering. We create pairs of independently heralded telecom-wavelength photons with high heralding efficiency (up to 65%) and brightness (4 kHz/mW), and we demonstrate a high lower bound for the indistinguishability (98.7 ± 0.2%) and spectral purity (90.7 ± 0.3%) via two-photon interference experiments.

OCIS codes: (270.0270) Quantum optics; (270.5585) Quantum information and processing; (270.6570) Squeezed states.

https://doi.org/10.1364/OPTICA.5.000514

Quantum photonics with single photons is a leading platform suitable for all aspects of quantum information processing—quantum computing and simulation, communication, and metrology. Multi-photon schemes such as recent proposals for loss-robust photonic cluster-state percolation [1] rely on a high number of successive two-photon interference events: any reduction in interference visibility leads to a drastic resource-cost increase in the required number of photon sources, detectors, and circuit complexity [2,3]. Since perfect interference can be achieved only with pure and indistinguishable photons [4], the development of high-quality single-photon sources is essential. A wide range of single-photon emitters is under development, typically classified into single-quantum emitters such as quantum dots [5] and parametric optical processes. The quality of photons and brightness of quantum dot sources is ever increasing; however, in many cases, parametric downconversion (PDC) in nonlinear crystals still provides a simpler, higher-quality solution especially at telecommunication wavelengths.

A central requirement for producing high-purity heralded photons via PDC is to remove the spectral correlations in the photon pairs that arise due to energy and momentum conservation: typically, narrow filters are employed to increase purity at the expense of brightness and heralding efficiency. This tradeoff can be overcome with three tricks known under the umbrella of "group-velocity matching" (GVM) [6–8]: (i) the group velocities of the PDC photons and pump laser need to be matched; (ii) the respective spectral bandwidths need to match; and (iii) the longitudinal nonlinearity profile of the PDC crystal needs to be Gaussian to remove residual correlations arising from the *sinc*-shaped phase-matching function (PMF) associated with standard crystals [9] (see Fig. 1). Techniques for tailoring crystal nonlinearities have only recently been adapted from the classical regime to the creation of spectrally pure photons [9–13]. Proof-of-principle demonstrations have verified that domain-engineered crystals can indeed create photons with approximated Gaussian spectra [9,11,14]. However, a reliable benchmark of the spectral purity achieved for single photons independently created in apodized crystals under GVM conditions has so far not been set.

Here, we implement a recently developed nonlinear crystal domain-engineering algorithm [10] in a group-velocity-matched regime at telecommunication wavelengths and demonstrate two-photon interference between heralded photons created in independent PDC processes. We simultaneously achieve high brightness, heralding efficiencies, signal-idler indistinguishability, and single-photon spectral purity without the use of lossy spectral filters. Importantly, our scheme creates symmetric heralding conditions, meaning that our photon sources are suitable not only for heralding single photons but also scalable to larger multi-photon protocols.

We first consider the first-order PDC bi-photon state:

$$|\psi_{\text{pair}}\rangle_{s,i} = \iint \mathrm{d}\omega_s \mathrm{d}\omega_i f(\omega_s,\omega_i)\hat{a}_s^\dagger(\omega_s)\hat{a}_i^\dagger(\omega_i)|0\rangle_{s,i}, \quad (1)$$

where s (i) denotes the signal (idler) photon. The joint spectral amplitude (JSA) $f(\omega_s,\omega_i)$ depends on the spectral properties of the pump and the PMF [6], which itself depends on the nonlinear

properties of the crystal. Whenever the detection of one photon of a pair heralds the presence of another, the spectral purity of the signal photon decreases as the signal-idler spectral correlations increase [7]. The JSA therefore has to be separable in order to generate pure photons.

To achieve that, we designed an apodized potassium titanyl phosphate (aKTP) crystal using the domain-engineering annealing algorithm introduced in Ref. [10], and we compare its performance with a periodically poled KTP (ppKTP). Starting from a seed poling period of 46.22 μm, our algorithm chooses each ferroelectric domain's orientation and width in order to shape the overall crystal PMF as a Gaussian function [Fig. 1(b)]. The crystals are phase matched for type-II PDC and produce two orthogonally polarized photons with central wavelength of 1550 nm and 1.5 nm bandwidth, estimated from the marginal spectral distributions of the $|JSA|^2$. Perfect GVM in KTP crystals is achieved when the pump has a Gaussian spectral envelope centered at 791 nm [7]: in these conditions, single-photon spectral purity from a standard ppKTP would be ~81.4%, compared to ~97.9% purity for our apodized crystal. Our experimental implementation slightly deviates from the ideal case though. First, mode-locked laser pulses have a sech^2-shaped intensity envelope. Second, the crystal length of 29 mm for the aKTP and 22 mm for the ppKTP is chosen to match the corresponding PMF full-width half-maximum (FWHM) of both crystals to a transform-limited sech^2 pulse centered at 775 nm and of 1.4 ps duration (defined as the FWHM of the pulse intensity envelope). However, our laser has a 1.7 ps pulse length, and the resulting JSA is slightly elliptical (Fig. 1). Under these conditions, we estimate single-photon purities of 80.1% and 95.3% for the standard and engineered crystals, respectively. These values define an upper bound for the experimentally achievable two-photon interference visibilities for independently heralded photons.

Our experimental setup is shown in Fig. 2. Our counting logic records the coincidences (cc) within a 1 ns time window between single photons (s_i) detected by the superconducting nanowire single-photon detectors (SNSPDs): we measure a source brightness of (11.25 ± 0.08) kHz/mW and (4.02 ± 0.04) kHz/mW of detected pairs for the ppKTP and the aKTP, respectively, and a four-photon rate for two independent sources of (1.52 ± 0.02) Hz/mW^2 and (0.19 ± 0.01) Hz/mW^2. We estimate a symmetric heralding efficiency $\eta = \text{cc}/(\sqrt{s_1 s_2})$ of 53% in the configuration used for the experiment, but a value of η up to 65% is achieved with the same crystals under loose focusing conditions [16], at the expense of brightness: this corresponds to a collection efficiency of 88.5% once detector efficiency (80%) and known optical losses of (7.6%) are accounted for.

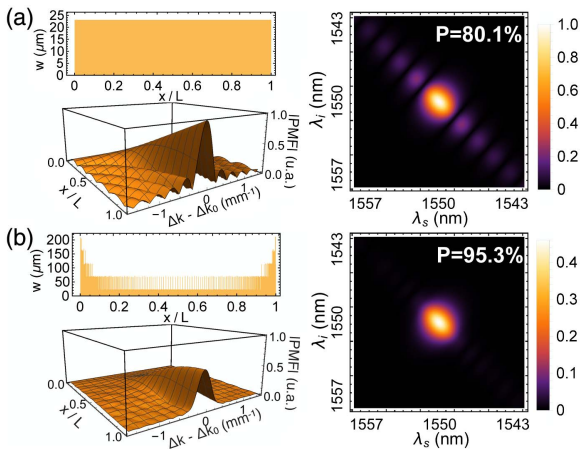


Fig. 1. Crystal domain-width (w) pattern (top-left), PMF along the crystal (bottom-left), and simulated JSA (right) for the ppKTP (a) and aKTP (b). The Δk depends on the signal-idler frequencies according to the Sellmeier equations used in Ref. [10]. The heralded-photon spectral purity is computed via a numerical Schmidt decomposition on the discretized JSA [15].

To estimate spectral photon purity from group-velocity-matched PDC sources, it is common practice to measure the bi-photon joint spectral intensity (JSI). The JSI can be measured with a pair of grating spectrometers, with dispersion spectroscopy [14], or via stimulated emission tomography [17,18]. However, the accuracy and precision of these measurements is often limited due to poor signal-to-noise ratios and a tradeoff between spectral range and resolution. Focusing on the central JSI peak in return for increased spectral resolution truncates correlations in the PMF side lobes, which are required for reliable purity estimation. To illustrate this for the standard ppKTP in Fig. 1, restricting the JSA to just the central peak increases the apparent purity calculated via the Schmidt decomposition from 80.1% to 93.2%. Furthermore, the JSI does not capture phase information. Performing the Schmidt decomposition on the square root of the JSI instead of the JSA for the same crystal yields a purity of 82.7% instead of 80.1%.

A more reliable benchmark for single-photon purity and indistinguishability is therefore the direct observation via two-photon interference. Interference between photons generated in the same PDC process gives an estimate of signal-idler indistinguishability [19]. More importantly, the two-photon interference visibility $(N_{\max} - N_{\min})/N_{\max}$ between heralded photons, where $N_{\max}$ ($N_{\min}$) is the maximum (minimum) number of coincident photon detections, corresponds to a direct measurement of single-photon purity [4].

This purity includes both the spectral as well as the photon-number degree of freedom. The photon number state of heralded PDC photons is typically mixed due to multi-photon emissions. While this is an intrinsic limitation of PDC, it can be mitigated to an arbitrary degree by multiplexing [20–23] and single-photon post-selection enabled by number-resolved detectors [24]. One can, however, obtain a lower bound on just the *spectral* purity by measuring interference versus pump power, as we outline below.

Omitting the spectral wavefunction, the PDC state in the Fock space is

$$|\psi_{\text{PDC}}\rangle = \sqrt{1 - |\lambda|^2} \sum_{n=0}^{\infty} \lambda^n |n\rangle_s |n\rangle_i, \tag{2}$$

where n is the photon number. The parameter λ relates to source brightness [20] and can be expressed as a function of the pump power P and of the constant τ, determined by the efficiency of the nonlinear process, the detection efficiency and optical loss in the setup: $\lambda = \sqrt{P\tau}$. Since perfect two-photon interference occurs when two and only two identical photons enter the 50-50 beam splitter (BS), all terms proportional to $|n > 1\rangle_s |n > 1\rangle_i$ in Eq. (2) compromise the interference visibility. In the limit of low pump power and negligible detector noise, the two-photon visibility

decreases linearly with increasing P (see Supplement 1 for details); therefore, we can extrapolate a visibility V_0 from measurements over a range of P (i.e., for a range of $\lambda \to 0$). V_0 provides a lower bound for the indistinguishability (in the case of signal-idler interference) and single-photon spectral purity (for two interfering heralded photons).

We first estimate the signal-idler indistinguishability by interfering photons produced in the same PDC process [see Fig. 2(c)] at different P. Figure 3(a) shows two-photon interference patterns for the ppKTP and the aKTP at low pump power without spectral filtering. Being in symmetric-GVM condition, the two-photon interference pattern can be approximated by the convolution of the PMF with itself [25]: as expected, it is almost triangular for the standard crystal [26], and Gaussian for the custom design. We find an indistinguishability V_0 of $(99.7 \pm 0.1)\%$ for the ppKTP and $(98.7 \pm 0.1)\%$ for the aKTP (see Supplement 1 for details). This signal-idler indistinguishability is, to our knowledge, the highest reported so far with an apodized crystal.

Ideally, measuring the spectral purity of a PDC photon requires the interference of two copies of the same photon [4]. The quantum state of a photon cannot be cloned, and the most faithful purity estimate is therefore obtained from interfering two photons emitted in short succession from the same crystal. In our setup, Fig. 2(b), we send the first heralded photon into a fiber delay line and a second into a shorter fiber before superposing them on a fiber beam splitter. This succeeds with probability 1/4, and we chose a delay of five pump pulses to exceed the ~60 ns SNSPD reset time. The two interfering photons are heralded by their respective twins, and four-photon coincidences are recorded. We extrapolate a V_0 of $(79.6 \pm 0.1)\%$ for the standard ppKTP, which matches theory expectations (see Fig. 1) and a V_0 of $(90.7 \pm 0.3)\%$ with the apodized crystals [see Fig. 3(b)]. We then interfere and detect photons produced by two different aKTP crystals [Fig. 2(d)] to show that our technique is feasible for multi-photon experiments. We also detect the idler photons and collect the overall number of fourfold coincidences from the four SNSPDs. In this configuration, we find a V_0 of $(89.8 \pm 0.2)\%$ [Fig. 3(b)].

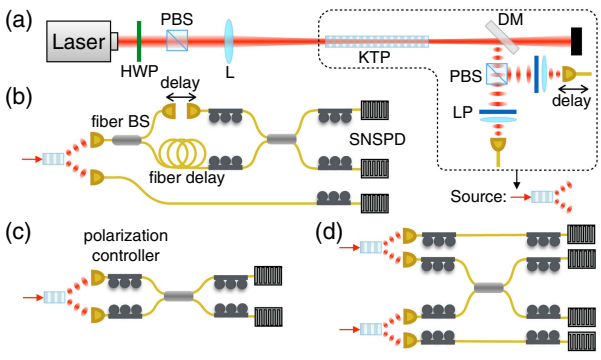


Fig. 2. Schematic of the experimental setup. (a) An 80 MHz repetition rate Ti-Sapphire laser is focused into the crystal where it generates 1550 nm PDC photons. These are split at a PBS and collected in single-mode fibers to be used in setups 2 (b)–(d). Laser light is removed with a dichroic mirror (DM) and long-pass filters (LP) The photons are detected by SNSPDs. We observe two-photon interference for: (b) photons created in the same setup at different times; (c) photons created in a single PDC process. (d) Photons created in two separate crystals.

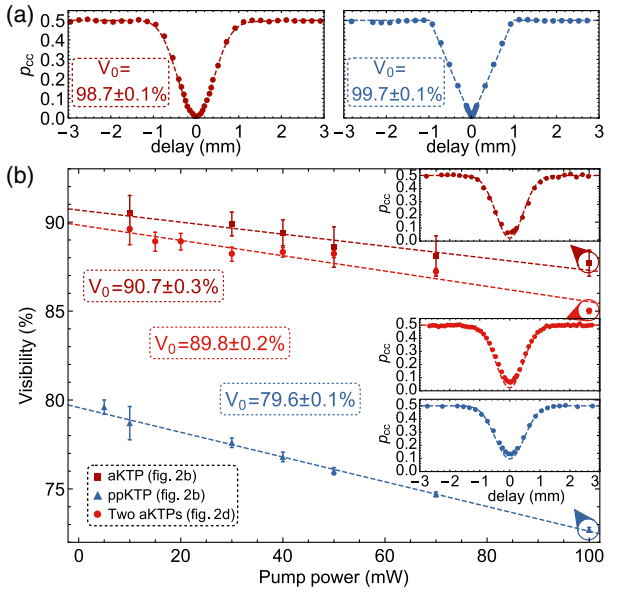


Fig. 3. (a) Two-photon interference as a function of temporal delay between photons generated by the same PDC process in the ppKTP (right) and the apodized crystal (left). Data are normalized against a coincidence probability of 1/2 outside the interference region. (b) Interference visibilities at different pump powers for the two experimental schemes in Figs. 2(b) and 2(d). The dashed lines are the simulated interference pattern obtained from the JSA in Fig. 1, while the visibilities are obtained from Gaussian fits. Statistical uncertainties on the visibilities of each interference experiment are estimated from 5000 samples of a Monte Carlo routine based on the Poissonian counting statistics of the experiment [27].

We can increase the quality of the photons produced with the aKTP, by applying "gentle" spectral filtering. We use a bandpass filter with a spectral transmission of the form $\exp[-\frac{(\omega-\omega_0)^4}{2\sigma^4}]$, centered at 1550 nm and a FWHM of 7.4 nm, which is roughly five times larger than the PDC bandwidth. This filter decreases heralding efficiency by no more than 1%—and in this configuration, we achieve a heralded-photon purity of $(92.7 \pm 0.2)\%$ and a signal-idler indistinguishability of $(99.7 \pm 0.1)\%$ (see Supplement 1 for details). This value is close to the maximum visibility we can achieve (99.8%) due to imperfect optics.

The V_0 corresponding to the apodized crystals shown in Fig. 3(a) are significantly higher than for the standard KTPs: however, they are still somewhat short of expectations (Fig. 1). Our fiber BS has a reflectivity (transmissivity) of 49.2% (50.8%), and the polarizing BS (PBS) leaks 0.5% of opposite polarized photons—a visibility decrease of ~0.2% for independent photon sources. Some degradation may be due to random duty-cycle errors occurring during crystal fabrication. To assess this error, we numerically vary each domain's width according to a Gaussian distribution with 1 μm FWHM and for each instance compute the JSA and corresponding photon purity. We find a decrease of the mean single-photon purity of about 0.3%, with a final value of $P = (95.0 \pm 0.2)\%$. Finally, the imperfect indistinguishability of the signal-idler photons, and its increase under gentle filtering suggests the presence of undesirable PDC generation far from the central JSA peak, which is not present in the standard ppKTP.

In Fig. 4, we assess the impact of spectral filtering on the heralding efficiency and the single-photon purity of our photon

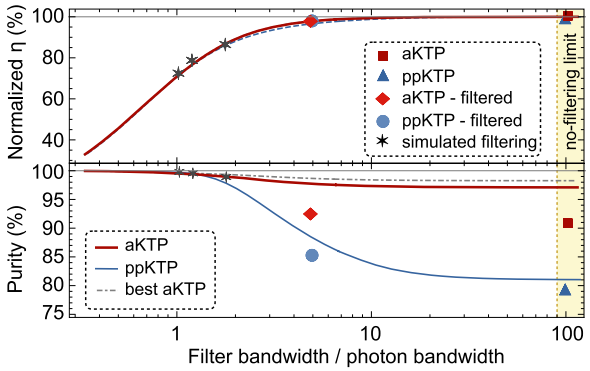


Fig. 4. Normalized heralding and purities for the ppKTP (blue) and the aKTP (red) under spectral filtering. The light-blue and light-red data points correspond to the ppKTP and aKTP with gentle filtering, while the dark gray stars represent three commercial bandpass filters (left to right: Iridian Spectral Technologies Ltd., Alluxa, Omega Optical Inc.) applied to the ppKTP. The dot-dashed gray line shows the simulated purity for a crystal tailored with optimal domain engineering [10].

sources. The normalized heralding represents the maximum heralding achievable, factoring out known losses, detection, and collection efficiency, while the x axis is the ratio between the filter and single-photon bandwidth. The data correspond to our setup, and the simulated heralding and purities hold in general for ppKTP/aKTP crystals of arbitrary length when group-velocity matched with a sech^2 pulse. We see a drastic tradeoff between spectral purity and heralding efficiency for photons created in standard ppKTP: A 99% purity can be achieved when a filter with twice the PDC bandwidth is applied to both photons. However, even ideal filters with 100% peak transmission would decrease the heralding efficiency to 80%, and the source brightness to 60%, which in a modest six-photon experiment would amount to a drop in observed rates to just 22%. In contrast, our apodized crystal sources operate in, or at least very close to, the "no-filtering" limit, overcoming this tradeoff. By fixing all known minor problems—fine tuning the domain-engineering algorithm, shaping a Gaussian pump pulse at 791 nm, and suppressing PDC noise—we are confident we can push the lower bound on spectral purity to at least 95% in the near future.

Funding. Engineering and Physical Sciences Research Council (EPSRC) (EP/L015110/1, EP/N002962/1).

Acknowledgment. The authors thank A. M. Brańczyk for useful discussions and A. Pickston and M. Ringbauer for experimental assistance.

See Supplement 1 for supporting content.

REFERENCES

1. M. Gimeno-Segovia, P. Shadbolt, D. E. Browne, and T. Rudolph, Phys. Rev. Lett. **115**, 020502 (2015).
2. Y. Li, S. D. Barrett, T. M. Stace, and S. C. Benjamin, Phys. Rev. Lett. **105**, 250502 (2010).
3. E. Meyer-Scott, N. Montaut, J. Tiedau, L. Sansoni, H. Herrmann, T. J. Bartley, and C. Silberhorn, Phys. Rev. A **95**, 061803 (2017).
4. A. M. Brańczyk, arXiv preprint arXiv:1711.00080 (2017).
5. P. Senellart, G. Solomon, and A. White, Nat. Nanotechnol. **12**, 1026 (2017).
6. W. P. Grice, A. B. U'Ren, and I. A. Walmsley, Phys. Rev. A **64**, 063815 (2001).
7. A. B. U'Ren, C. Silberhorn, R. Erdmann, K. Banaszek, W. P. Grice, I. A. Walmsley, and M. G. Raymer, arXiv preprint quant-ph/0611019 (2006).
8. P. J. Mosley, J. S. Lundeen, B. J. Smith, and I. A. Walmsley, New J. Phys. **10**, 093011 (2008).
9. A. M. Brańczyk, A. Fedrizzi, T. M. Stace, T. C. Ralph, and A. G. White, Opt. Express **19**, 55 (2011).
10. F. Graffitti, D. Kundys, D. T. Reid, A. M. Brańczyk, and A. Fedrizzi, Quantum Sci. Technol. **2**, 035001 (2017).
11. P. B. Dixon, J. H. Shapiro, and F. N. C. Wong, Opt. Express **21**, 5879 (2013).
12. A. Dosseva, Ł. Cincio, and A. M. Brańczyk, Phys. Rev. A **93**, 013801 (2016).
13. J.-L. Tambasco, A. Boes, L. G. Helt, M. J. Steel, and A. Mitchell, Opt. Express **24**, 19616 (2016).
14. C. Chen, C. Bo, M. Y. Niu, F. Xu, Z. Zhang, J. H. Shapiro, and F. N. C. Wong, Opt. Express **25**, 7300 (2017).
15. F. Laudenbach, H. Hübel, M. Hentschel, P. Walther, and A. Poppe, Opt. Express **24**, 2712 (2016).
16. L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam, Phys. Rev. Lett. **115**, 250402 (2015).
17. M. Liscidini and J. E. Sipe, Phys. Rev. Lett. **111**, 193602 (2013).
18. A. Eckstein, G. Boucher, A. Lemaître, P. Filloux, I. Favero, G. Leo, J. E. Sipe, M. Liscidini, and S. Ducci, Laser Photon. Rev. **8**, L76 (2014).
19. V. Giovannetti, L. Maccone, J. H. Shapiro, and F. N. C. Wong, Phys. Rev. A **66**, 043813 (2002).
20. M. A. Broome, M. P. Almeida, A. Fedrizzi, and A. G. White, Opt. Express **19**, 22698 (2011).
21. M. J. Collins, C. Xiong, I. H. Rey, T. D. Vo, J. He, S. Shahnia, C. Reardon, T. F. Krauss, M. J. Steel, A. S. Clark, and B. J. Eggleton, Nat. Commun. **4**, 2582 (2013).
22. C. Xiong, X. Zhang, Z. Liu, M. J. Collins, A. Mahendra, L. G. Helt, M. J. Steel, D.-Y. Choi, C. J. Chae, P. H. W. Leong, and B. J. Eggleton, Nat. Commun. **7**, 10853 (2016).
23. F. Kaneda, F. Xu, J. Chapman, and P. G. Kwiat, Optica **4**, 1034 (2017).
24. V. D'Auria, O. Morin, C. Fabre, and J. Laurat, Eur. Phys. J. D **66**, 249 (2012).
25. M. Barbieri, E. Roccia, L. Mancino, M. Sbroscia, I. Gianani, and F. Sciarrino, Sci. Rep. **7**, 7247 (2017).
26. A. Fedrizzi, T. Herbst, M. Aspelmeyer, M. Barbieri, T. Jennewein, and A. Zeilinger, New J. Phys. **11**, 103052 (2009).
27. N. K. Langford, "Encoding, manipulating and measuring quantum information in optics," Ph.D. thesis (University of Queensland, 2007).

Appendix B

Assisted Macroscopic Quantumness

In this Appendix, I report on an experimental result possibly relevant in relation to the observer definition given in Sec 4.4, as it was used to support the results of Chapter 4. That definition proposes a prescription to determine whether a physical system can count as an observer or not, and in particular it lacks of any reference to the observer's size. On one hand, this should not be surprising as quantum mechanics does not present any reference to the size of physical systems, and accordingly there should not be any reference to the size of physical systems in an observer definition. On the other hand, the absence of experimental observations showing quantum effects at any scale, might suggest that if a meaningful notion of macro-scale is given, then quantum mechanics might be superfluous when applied to systems beyond such macro-scale. Therefore, denying our definition of observer and replacing it with one taking into account the size of a physical system, it is a valid approach. In this Appendix, the experiment presented supports the theory in Ref [94] where it is claimed that the existence of such macro-scale is unjustifiable from an information-theoretic perspective.

In the following results, I contributed with the preparation and characterisation of the experimental setup. I then partially contributed with the data acquisition. The theoretical background was firstly introduced by Farid Shahandeh and lately experimentally tested by our group, leading to a joint work.

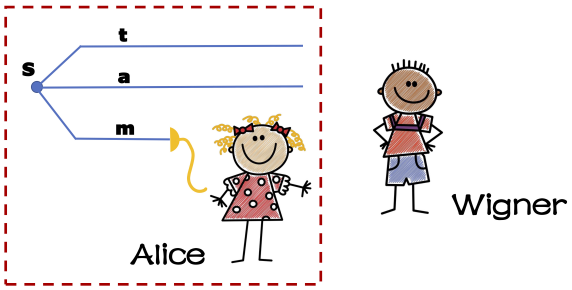


Figure B.1: **The schematic of our protocol.** A source **S** produces an entangled pair in modes **t** and **m** and an ancilla photon in mode **a**. Photons **a** and **t** then interact to produce the state of Eq. (B.1). The state undergoes partial decoherence before the qubit in mode **m** is measured by the macroscopic observer Alice, who also undergoes decoherence. Wigner, outside Alice's laboratory, concludes that Alice and any of the two qubits **a** or **t** are jointly entangled with the other qubit, while there is no entanglement between the qubits **a** and **t** alone.

B.0.1 Theory Background

A commonly conjectured roadblock for macroscopic quantum effects is quantum decoherence related to the size of the considered system [207, 208]. Loosely speaking, the larger the system is (according to some appropriate notion of macroscopicity [209–215]), the harder it is to isolate it from interactions with the environment. Such interactions, in turn, destroy the coherence of the system, hence, no quantum property of a *sufficiently large* system can be observed unless via extremely high-precision measurements [209, 212]. In other words, it is assumed that there exists a "macro-scale" beyond which physical systems can be analyzed without any reference to the quantum formalism.

Here, this view is challenged by showing that a macroscopic system (that is a system being subject to full decoherence) assisted by a second system can be proved to be entangled with another system, we call this behaviour "assisted macroscopic quantumness". We set the scene as in a Wigner's friend experiment, with the crucial difference that the observer is not assumed to preserve quantum coherence, and analyze Wigner's perspective, see Fig. B.1. In our variant, Wigner's friend (Alice) is in possession of two particles, labeled **a** and **t**, and measures a particle in the mode **m**. We find that, even in the presence of decoherence and regardless of its dynamics, the joint subsystem of Alice and particle **t** exhibits entanglement with particle **a**, while there is no entanglement in any pair of subsystems alone. Consequently, as far as the information content of Alice is concerned, she constitutes a quantum system

in assistance with particle $\mathbf{t}$ regardless of her size. More specifically, Wigner has to use the quantum formalism to describe the entanglement in this particular partition, independent of our choice of interpretation of quantum theory. Hence, there seems to be no escape from the conclusion that Alice, despite being a macroscopic observer by any sensible definition, is an *informationally indispensable* part of the quantum system.

Consider a source of photons that produces a three-mode entangled state of the form

$$|\Phi\rangle_{\mathbf{atm}} = \frac{|\Psi_+\rangle_{\mathbf{at}}|0\rangle_{\mathbf{m}}+|\Psi_-\rangle_{\mathbf{at}}|1\rangle_{\mathbf{m}}}{\sqrt{2}} \tag{B.1}$$

where $|\Psi_\pm\rangle_{\mathbf{at}}=(|01\rangle_{\mathbf{at}} \pm |10\rangle_{\mathbf{at}})/\sqrt{2}$. We assume now decoherence relative to the system $\mathbf{m}$ that will eventually be measured by the macroscopic observer Alice, while making the empirically justified assumption that the coherence between the remaining qubit systems can be maintained. The resulting state from Alice perspective after decoherence is given by

$$\hat{\varrho}^{(\mathbf{A})}_{\mathbf{atm}}= \left(|\Psi_+\rangle_{\mathbf{at}}\langle\Psi_+|\otimes|0\rangle_{\mathbf{m}}\langle 0|+|\Psi_-\rangle_{\mathbf{at}}\langle\Psi_-|\otimes|1\rangle_{\mathbf{m}}\langle 1|\right)/2. \tag{B.2}$$

A crucial observation at this point is that the state assigned by Alice features no entanglement between any pair of qubits, i.e. within partitions $(\mathbf{a}|\mathbf{t})$, $(\mathbf{a}|\mathbf{m})$, and $(\mathbf{m}|\mathbf{t})$. Nonetheless, Alice can verify that the state in Eq. (B.2) is quantum by measuring the negativity of the state within partitions $(\mathbf{am}|\mathbf{t})$ and $(\mathbf{a}|\mathbf{tm})$, implying that two of the qubits are entangled with the other qubit in these particular partitions. Alice then performs a measurement on the qubit in mode $\mathbf{m}$ to update her knowledge of the ancilla and target ($\mathbf{a}$ and $\mathbf{t}$) subsystems.

From Wigner's perspective, outside the closed laboratory, the situation is different. Following the quantum prescription, Wigner assigns the state $|\overline{\Phi}\rangle_{\mathbf{atmA}} = (|\Psi_+\rangle_{\mathbf{at}}|0\rangle_{\mathbf{m}}|\xi\rangle_{\mathbf{A}} + |\Psi_-\rangle_{\mathbf{at}}|1\rangle_{\mathbf{m}}|\zeta\rangle_{\mathbf{A}})/\sqrt{2}$, where $|\xi\rangle_{\mathbf{A}}$ and $|\zeta\rangle_{\mathbf{A}}$ are the memory states if Alice encoding her measurement result. Hence, by taking into account the decoherence of the initial state, and that Alice undergoes decoherence, Wigner assigns to the remaining ancilla-target-Alice system after Alice's measurement a state of the form

$$\hat{\varrho}^{(\mathbf{W})}_{\mathbf{atA}} = \left(|\Psi_+\rangle_{\mathbf{at}}\langle\Psi_+|\otimes\hat{\tau}_{\mathbf{A}} + |\Psi_-\rangle_{\mathbf{at}}\langle\Psi_-|\otimes\hat{\upsilon}_{\mathbf{A}}\right)/2. \tag{B.3}$$

We assume that the system in mode $\mathbf{m}$ is destroyed by Alice's measurement, but non-destructive measurements (e.g. in spin systems) would lead to an equivalent description. The states $\hat{\tau}_{\mathbf{A}}$ and $\hat{v}_{\mathbf{A}}$ represent Alice's state after decoherence. Notably by calculating the negativity (see Sec 2.6 for its definition) of the state in Eq. (B.3) we obtain

$$N[\hat{\varrho}^{(\mathbf{W})}_{\mathbf{atA}};(\mathbf{aA}|\mathbf{t})] = N[\hat{\varrho}^{(\mathbf{W})}_{\mathbf{atA}};(\mathbf{a}|\mathbf{tA})] = \frac{\|\hat{\tau}_{\mathbf{A}}-\hat{v}_{\mathbf{A}}\|_1}{4}. \tag{B.4}$$

where $\|\cdot\|_1$ is the ℓ_1-norm, i.e. the sum of the absolute values of the eigenvalues. Wigner must therefore conclude, independent of his of interpretation of quantum theory, that: (i) Alice is part of a large entangled state within partitions $(\mathbf{aA}|\mathbf{t})$ and $(\mathbf{a}|\mathbf{tA})$; (ii) the amount of entanglement within both partitions is determined by the distinguishability of Alice's memory states; (iii) the entanglement *is not* merely due to qubits, as Alice is *necessary* for obtaining any entanglement. In other words, if Alice is disregarded by tracing her out, there is no entanglement within the remaining system $(\mathbf{a}|\mathbf{t})$. Importantly, both of the states $\hat{\varrho}^{(\mathbf{A})}_{\mathbf{atm}}$ and $\hat{\varrho}^{(\mathbf{W})}_{\mathbf{atA}}$ are entangled on equal footings, since there is nothing within the theory that makes an informational difference between the $\mathbf{m}$-qubit and Alice. Consequently, the placement of the system-apparatus cut is critical in our experiment in the sense that the observations made by Wigner and Alice remain incompatible, even under full decoherence. Only when Alice is admitted a quantum treatment can the entanglement of the joint system be revealed.

B.0.2 Experimental Results

Experimentally, Wigner can verify the entanglement of the state in Eq. (B.3) by performing measurements on the ancilla and target qubits and asking Alice about her measurement results. As shown in Ref [94] this can be achieved with the two witnesses

$$\begin{aligned}\hat{W}_1 &= |\Phi_+\rangle_{\mathbf{at}}\langle\Phi_+|^{\mathsf{T}_{\mathbf{t}}} \otimes |\text{“up”}\rangle_{\mathbf{A}}\langle\text{“up”}|,\\ \hat{W}_2 &= |\Phi_+\rangle_{\mathbf{at}}\langle\Phi_+|^{\mathsf{T}_{\mathbf{t}}} \otimes |\text{“down”}\rangle_{\mathbf{A}}\langle\text{“down”}|,\end{aligned} \tag{B.5}$$

where $^{\mathsf{T}_{\mathbf{t}}}$ denotes partial transposition with respect to subsystem $\mathbf{t}$ and $|\Phi_\pm\rangle_{\mathbf{at}} = (|00\rangle_{\mathbf{at}} \pm |11\rangle_{\mathbf{at}})/\sqrt{2}$. A given state $\hat{\varrho}^\star$ is entangled within partitions $(\mathbf{aA}|\mathbf{t})$ and $(\mathbf{a}|\mathbf{tA})$ if

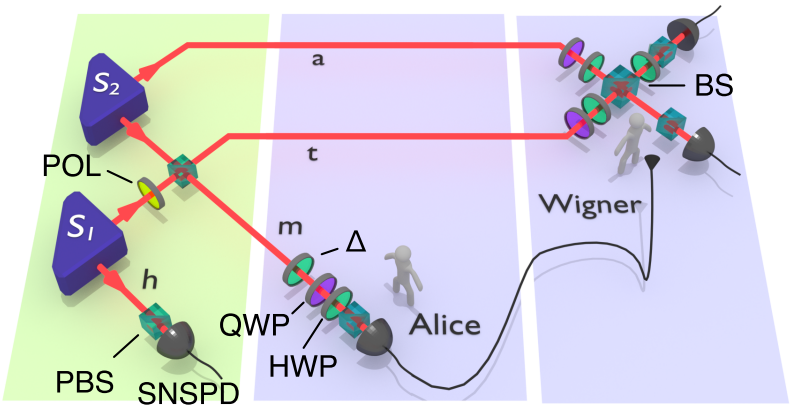


Figure B.2: **Experimental setup**. The three-mode entangled state of Eq. (B.1) is generated in modes **m**, **a**, and **t** using two Sagnac-based spontaneous parametric downconversion sources [46], of which S_1 is set to prepare the entangled state $|\Psi_-\rangle$ and S_2 the separable state $|+\rangle|0\rangle$ using polarizers (POL). The photons are then combined in a type-I fusion gate [47] implemented through a polarizing beam splitter (PBS). One of the 4 emitted photons is detected in the auxiliary mode **h** to provide a heralding signal for the state preparation. In order to simulate environmental decoherence, the so-generated state can be continuously dephased up to the state of Eq. (B.2), by imparting phase flips on mode **m** to an appropriate fraction of the experimental runs using a half-waveplate (HWP), denoted Δ. Alice then measures the qubit in mode **m** using a set of HWP and quarter-waveplates (QWP) and PBS before detecting the photon using superconducting nanowire detectors (SNSPD). In order to measure the witnesses of Eq. (B.5), arbitrary Bell-basis measurements on modes **at** are achieved using non-classical interference in a 50/50 beamsplitter (BS) combined with HWP and QWP rotations and coincidence detection.

$\mathrm{Tr}\hat{\varrho}^{\star}\hat{W}_1<0$, or $\mathrm{Tr}\hat{\varrho}^{\star}\hat{W}_2<0$. This witnessing procedure is operationally equivalent to Wigner asking Alice about her memory and measuring $|\Phi_+\rangle_{\mathbf{at}}\langle\Phi_+|^{\mathsf{T}_\mathbf{t}}$ for the ancilla-target two-qubit subsystem. Note that Alice may use the same recipe to witness the entanglement of her state by substituting "asking Alice" with "measurements in the computational basis on mode **m**". We implemented the modified Wigner's friend scenario in a photonic experiment as depicted in Fig. B.2 using two independent photon-pair sources and a type-I fusion gate [47]. The reader is referred to Section 4.4 for a detailed description of the experimental components, as the setup employed for the results shown here is a subpart of the more complex setup employed for the main results of this chapter. We measured the witnesses in Eq. (B.5), and verified Wigner's conclusion about the entanglement of his state $\hat{\varrho}^{(\mathbf{W})}_{\mathbf{atA}}$. In order to consider the effects of decoherence, we experimentally implement a single-qubit dephasing channel $\rho \mapsto (1-\frac{\eta}{2})\rho + \frac{\eta}{2}\sigma_z\rho\sigma_z$ on mode **m** before Alice's measurement via random phase flips, see Fig. B.2. This allows us to continuously

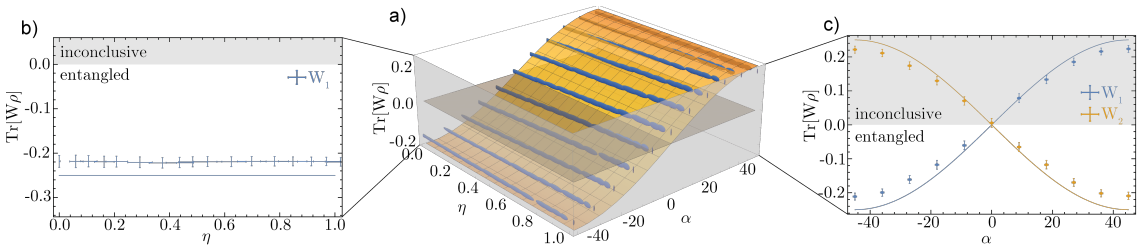


Figure B.3: **Experimental results. a)** Measured expectation values $\langle \hat{W}_1 \rangle$ for the witness $\hat{W}_1$ as a function of the amount of dephas5ing η and the distinguishability of Alice's measurement results as measured by α. The orange surface represents the theory prediction, the gray plane indicates the boundary below which $\hat{W}_1$ certifies the presence of entanglement in the partitions $(\mathbf{a}|\mathbf{tA})$ and $(\mathbf{t}|\mathbf{aA})$. The size of the blue data points in the 3-dimensional plot correspond to 3-sigma statistical uncertainty obtained from a Monte Carlo routine simulating the Poissonian counting statistics. **b)** Measured expectation values $\langle \hat{W}_1 \rangle$ for different amounts of dephasing in the limiting case of perfect distinguishability ($\alpha = 45°$). **c)** Measured expectation values $\langle \hat{W}_1 \rangle$ (blue) and $\langle \hat{W}_2 \rangle$ (orange) for different distinguishability of Alice's measurements in the case of full dephasing ($\eta = 1$). The gray shaded area indicates the region where the witness is inconclusive, while the white area is where either witness certifies entanglement. All error bars represent 3-sigma statistical uncertainty regions.

tune the state before Alice's measurement from the pure state of Eq. (B.1) to the fully decohered state of Eq. (B.2). The results of Fig. B.3 show that the observed entanglement is independent of the strength η of the decoherence applied to the state. This clearly shows that Alice remains an indispensable part of an entangled state even under full decoherence and independent of any micro-macro distinction. Additionally, we considered the effects of imperfect distinguishability of Alice's results, by having her implement a measurement described by the non-orthogonal projectors $\{\cos(\pi/4 \pm \alpha)|0\rangle + \sin(\pi/4 \pm \alpha)|1\rangle\}$ on the qubit in mode $\mathbf{m}$, see Fig. B.2. For $\alpha = \pm\,\pi/4$ this implements the ideal measurement of qubit $\mathbf{m}$ in the $\{|0\rangle, |1\rangle\}$ basis, while for α=0 the measurement reveals no information about the qubit's polarization state. This measurement thus enables us to study the case where Alice's memory does not allow for a perfect identification of the state in mode $\mathbf{m}$, where the distinguishability of her measurement results is given by $\|\hat{\tau}_{\mathbf{A}} - \hat{v}_{\mathbf{A}}\|_1 = |\sin[2\alpha]|$. To measure the entanglement witness of Eq. (B.5), from Wigner's perspective, we measured the two qubits in modes $\mathbf{a}$ and $\mathbf{t}$ and asked Alice for her observed results. The results in Fig. B.3 indicate that either of the witness $\hat{W}_1$ or $\hat{W}_2$ certifies the presence of entanglement in the partitions $(\mathbf{a}|\mathbf{tA})$ and $(\mathbf{t}|\mathbf{aA})$ for all non-zero values

of distinguishability of Alice's measurement results (i.e. $\alpha \neq 0$).

In conclusion, we shown that even under full decoherence of Wigner's friend—which from the point of view of the standard experiment destroys all quantum effects—a careful information-theoretic analysis reveals residual entanglement. This entanglement, as we show, depends crucially on the information held by Wigner's friend and can thus only be revealed when the observer is taken into account and giving a quantum description. In relation to the photonic observers employed for the main result of this chapter, it suggests that they can remain valid observers even if they undergo full-decoherence after establishing a fact.

Bibliography

[1] Daniel Gottesman. Stabilizer codes and quantum error correction. *arXiv preprint quant-ph/9705052*, 1997.

[2] Robert Raussendorf, Daniel E Browne, and Hans J Briegel. Measurement-based quantum computation on cluster states. *Physical Review A*, 68(2):022312, 2003.

[3] Hans J Briegel, David E Browne, Wolfgang Dür, Robert Raussendorf, and M Nest. Measurement-based quantum computation. *Nature Physics*, 5(19-26), 2009.

[4] Géza Tóth and Otfried Gühne. Entanglement detection in the stabilizer formalism. *Physical Review A*, 72(2):022340, 2005.

[5] Keisuke Fujii. *Quantum Computation with Topological Codes: from qubit to topological fault-tolerance*, volume 8. Springer, 2015.

[6] Michael A Nielsen and Isaac Chuang. *Quantum computation and quantum information*. AAPT, 2002.

[7] Pieter Kok and Brendon W Lovett. *Introduction to optical quantum information processing*. Cambridge university press, 2010.

[8] Marc Hein, Jens Eisert, and Hans J Briegel. Multiparty entanglement in graph states. *Physical Review A*, 69(6):062311, 2004.

[9] Marc Hein, Wolfgang Dür, Jens Eisert, Robert Raussendorf, M Nest, and H-J Briegel. Entanglement in graph states and its applications. *arXiv preprint quant-ph/0602096*, 2006.

[10] Daniel Gottesman. The heisenberg representation of quantum computers. *arXiv preprint quant-ph*, 9807006, 1998.

[11] Maarten Van den Nest, Jeroen Dehaene, and Bart De Moor. Graphical description of the action of local clifford transformations on graph states. *Physical Review A*, 69(2):022316, 2004.

[12] Simon Anders and Hans J Briegel. Fast simulation of stabilizer circuits using a graph-state representation. *Physical Review A*, 73(2):022334, 2006.

[13] Jeremy C Adcock, Sam Morley-Short, Axel Dahlberg, and Joshua W Silverstone. Mapping graph state orbits under local complementation. *arXiv preprint arXiv:1910.03969*, 2019.

[14] GM D'Ariano, L Maccone, and MGA Paris. Orthogonality relations in quantum tomography. *Physics Letters A*, 276(1-4):25–30, 2000.

[15] Roger Penrose. On best approximate solutions of linear matrix equations. *Mathematical Proceedings of the Cambridge Philosophical Society*, 52(1):17–19, 1956.

[16] Zdenek Hradil. Quantum-state estimation. *Physical Review A*, 55(3):R1561, 1997.

[17] Daniel FV James, Paul G Kwiat, William J Munro, and Andrew G White. On the measurement of qubits. *Asymptotic Theory of Quantum Statistical Inference: Selected Papers*, pages 509–538, 2005.

[18] Michael Grant and Stephen Boyd. CVX: Matlab software for disciplined convex programming, version 2.1. `http://cvxr.com/cvx`, March 2014.

[19] Richard Jozsa. Fidelity for mixed quantum states. *Journal of Modern Optics*, 41(12):2315–2323, 1994.

[20] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81(2):865, 2009.

[21] Otfried Gühne and Géza Tóth. Entanglement detection. *Physics Reports*, 474(1-6):1–75, 2009.

[22] Scott Hill and William K Wootters. Entanglement of a pair of quantum bits. *Physical Review Letters*, 78(26):5022, 1997.

[23] Pranaw Rungta, Vladimir Bužek, Carlton M Caves, Mark Hillery, and Gerard J Milburn. Universal state inversion and concurrence in arbitrary dimensions. *Physical Review A*, 64(4):042315, 2001.

[24] Karol Zyczkowski, Pawel Horodecki, Anna Sanpera, and Maciej Lewenstein. On the volume of the set of mixed entangled states. *arXiv preprint quant-ph/9804024*, 1998.

[25] Pascale Senellart, Glenn Solomon, and Andrew White. High-performance semiconductor quantum-dot single-photon sources. *Nature Nanotechnology*, 12(11):1026, 2017.

[26] H Jeff Kimble, Mario Dagenais, and Leonard Mandel. Photon antibunching in resonance fluorescence. *Physical Review Letters*, 39(11):691, 1977.

[27] Frank Diedrich and Herbert Walther. Nonclassical radiation of a single stored ion. *Physical Review Letters*, 58(3):203, 1987.

[28] Th Basché, WE Moerner, M Orrit, and H Talon. Photon antibunching in the fluorescence of a single dye molecule trapped in a solid. *Physical Review Letters*, 69(10):1516, 1992.

[29] Hui Wang, Yu-Ming He, T-H Chung, Hai Hu, Ying Yu, Si Chen, Xing Ding, M-C Chen, Jian Qin, Xiaoxia Yang, et al. Towards optimal single-photon sources from polarized microcavities. *Nature Photonics*, 13(11):770–775, 2019.

[30] Hui Wang, Hai Hu, T-H Chung, Jian Qin, Xiaoxia Yang, J-P Li, R-Z Liu, H-S Zhong, Y-M He, Xing Ding, et al. On-demand semiconductor source of entangled photons which simultaneously has high fidelity, efficiency, and indistinguishability. *Physical Review Letters*, 122(11):113602, 2019.

[31] Rodney Loudon. *The quantum theory of light*. OUP Oxford, 2000.

[32] Robert W Boyd. *Nonlinear optics*. Academic press, 2003.

[33] Georg Harder. *Optimized down-conversion source and state-characterization tools for quantum optics*. PhD thesis, 2016.

[34] Valentin G Dmitriev, Gagik G Gurzadyan, and David N Nikogosyan. *Handbook of nonlinear optical crystals*, volume 64. Springer, 2013.

[35] Agata M Brańczyk, TC Ralph, Wolfram Helwig, and Christine Silberhorn. Optimized generation of heralded fock states using parametric down-conversion. *New Journal of Physics*, 12(6):063001, 2010.

[36] Evan Meyer-Scott, Nicola Montaut, Johannes Tiedau, Linda Sansoni, Harald Herrmann, Tim J Bartley, and Christine Silberhorn. Filtering is not enough for pure, efficient photon pairs. *arXiv preprint arXiv:1702.05501*, 2017.

[37] Francesco Graffitti, Dmytro Kundys, Derryck T Reid, Agata M Brańczyk, and Alessandro Fedrizzi. Pure down-conversion photons through sub-coherence length domain engineering. *Quantum Science Technology 2 035001*, 2017.

[38] Agata M Brańczyk, Alessandro Fedrizzi, Thomas M Stace, Tim C Ralph, and Andrew G White. Engineered optical nonlinearity for quantum light sources. *Optics Express*, 19(1):55–65, 2011.

[39] Changchen Chen, Cao Bo, Murphy Yuezhen Niu, Feihu Xu, Zheshen Zhang, Jeffrey H Shapiro, and Franco NC Wong. Efficient generation and characterization of spectrally factorable biphotons. *Optics Express*, 25(7):7300–7312, 2017.

[40] P Ben Dixon, Jeffrey H Shapiro, and Franco NC Wong. Spectral engineering by gaussian phase-matching for quantum photonics. *Optics Express*, 21(5):5879–5890, 2013.

[41] DT Reid. Engineered quasi-phase-matching for second-harmonic generation. *Journal of Optics A: Pure and Applied Optics*, 5(4):S97, 2003.

[42] Ryan S Bennink. Optimal collinear gaussian beams for spontaneous parametric down-conversion. *Physical Review A*, 81(5):053805, 2010.

[43] P Ben Dixon, Danna Rosenberg, Veronika Stelmakh, Matthew E Grein, Ryan S Bennink, Eric A Dauler, Andrew J Kerman, Richard J Molnar, and Franco NC Wong. Heralding efficiency and correlated-mode coupling of near-ir fiber-coupled photon pairs. *Physical Review A*, 90(4):043804, 2014.

[44] Pieter Kok, W. J. Munro, Kae Nemoto, T. C. Ralph, Jonathan P. Dowling, and G. J. Milburn. Linear optical quantum computing with photonic qubits. *Review of Modern Physics*, 79:135–174, Jan 2007.

[45] M. A. Broome, M. P. Almeida, A. Fedrizzi, and A. G. White. Reducing multi-photon rates in pulsed down-conversion by temporal multiplexing. *Opt. Express*, 19(23):22698–22708, Nov 2011.

[46] Alessandro Fedrizzi, Thomas Herbst, Andreas Poppe, Thomas Jennewein, and Anton Zeilinger. A wavelength-tunable fiber-coupled source of narrowband entangled photons. *Opt. Express*, 15(23):15377–15386, 2007.

[47] Daniel E Browne and Terry Rudolph. Resource-efficient linear optical quantum computation. *Physical Review Letters*, 95(1):010501, 2005.

[48] Vittorio Degiorgio. Phase shift between the transmitted and the reflected optical fields of a semireflecting lossless mirror is $\pi/2$. *American Journal of Physics*, 48(1):81–81, 1980.

[49] Nathan K Langford, TJ Weinhold, R Prevedel, KJ Resch, Alexei Gilchrist, JL O'Brien, GJ Pryde, and AG White. Demonstration of a simple entangling optical gate and its use in bell-state analysis. *Physical Review Letters*, 95(21):210504, 2005.

[50] Chao Zhang, Yun-Feng Huang, Bi-Heng Liu, Chuan-Feng Li, and Guang-Can Guo. Experimental generation of a high-fidelity four-photon linear cluster state. *Physical Review A*, 93(6):062329, 2016.

[51] Han-Sen Zhong, Yuan Li, Wei Li, Li-Chao Peng, Zu-En Su, Yi Hu, Yu-Ming He, Xing Ding, Weijun Zhang, Hao Li, et al. 12-photon entanglement and scalable scattershot boson sampling with optimal entangled-photon pairs from parametric down-conversion. *Physical Review Letters*, 121(25):250505, 2018.

[52] Jeremy C Adcock, Sam Morley-Short, Joshua W Silverstone, and Mark G Thompson. Hard limits on the postselectability of optical graph states. *Quantum Science and Technology*, 4(1):015010, 2018.

[53] Massimiliano Proietti, Alexander Pickston, Francesco Graffitti, Peter Barrow, Dmytro Kundys, Cyril Branciard, Martin Ringbauer, and Alessandro Fedrizzi. Experimental test of local observer independence. *Science Advances*, 5(9):eaaw9832, 2019.

[54] John Von Neumann. *Mathematical Foundations of Quantum Mechanics: New Edition*. Princeton University Press, 2018.

[55] Paul Adrien Maurice Dirac. *The principles of quantum mechanics*. Number 27. Oxford University Press, 1981.

[56] Giancarlo Ghirardi. Collapse theories. *The Stanford Encyclopedia of Philosophy*, 2018.

[57] John Bell. Against 'measurement'. *Physics world*, 3(8):33, 1990.

[58] Wayne Myrvold. Philosophical issues in quantum theory. *The Stanford Encyclopedia of Philosophy*, 2018.

[59] Louis De Broglie. Nouvelle dynamique des quanta. *Rapport et discussions du Vê Conseil de Physique Solvay (1928)*.

[60] David Bohm. A Suggested Interpretation of the Quantum Theory in Terms of "Hidden" Variables. I & II. *Physical Review*, 85(2):166–193, 1952.

[61] Hugh III Everett. "Relative State" Formulation of Quantum Mechanics. *Rev. Mod. Phys.*, 29(3):454–462, 1957.

[62] Hugh Everett and Jeffrey A Barrett. *The Everett interpretation of quantum mechanics: Collected works 1955-1980 with commentary*. Princeton University Press, 2012.

[63] David Wallace. *The emergent multiverse: Quantum theory according to the Everett interpretation*. Oxford University Press, 2012.

[64] Simon Saunders, Jonathan Barrett, Adrian Kent, and David Wallace. *Many worlds?: Everett, quantum theory, & reality.* Oxford University Press, 2010.

[65] G. C. Ghirardi, A. Rimini, and T. Weber. Unified dynamics for microscopic and macroscopic systems. *Phys. Rev. D*, 34(2):470–491, 1986.

[66] Philip Pearle. Reduction of the state vector by a nonlinear schrödinger equation. *Physical Review D*, 13(4):857, 1976.

[67] E.P. Wigner. Remarks on the Mind-Body Question. *The Scientist Speculates (1961*, pages 284–302.

[68] David Deutsch. Quantum theory as a universal physical theory. *Int. J. Theor. Phys.*, 24(1):1–41, 1985.

[69] John S. Bell. On the Einstein Podolsky Rosen Paradox. *Physics*, 1(3):195–200, 1964.

[70] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777, 1935.

[71] Niels Bohr. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 48(8):696, 1935.

[72] John S. Bell. The theory of local beables. *Epistemic Letters*, 9:11–24, 1976.

[73] Howard M Wiseman and Eric G Cavalcanti. Causarum investigatio and the two bell's theorems of john bell. *Quantum [Un] Speakables II (2017*, pages 119–142.

[74] John Clauser, Michael Horne, Abner Shimony, and Richard Holt. Proposed Experiment to Test Local Hidden-Variable Theories. *Physical Review Letters*, 23(15):880–884, 1969.

[75] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Reviews of Modern Physics*, 86(2):419, 2014.

[76] Stuart J. Freedman and John F. Clauser. Experimental test of local hidden-variable theories. *Phys. Rev. Lett.*, 28:938–941, Apr 1972.

[77] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental tests of realistic local theories via bell's theorem. *Physical Review Letters*, 47:460–463, Aug 1981.

[78] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: A new violation of bell's inequalities. *Physical Review Letters*, 49:91–94, Jul 1982.

[79] John F. Clauser and Michael A. Horne. Experimental consequences of objective local theories. *Phys. Rev. D*, 10:526–535, Jul 1974.

[80] Philip M. Pearle. Hidden-variable example based upon data rejection. *Phys. Rev. D*, 2:1418–1425, Oct 1970.

[81] Mary A Rowe, David Kielpinski, Volker Meyer, Charles A Sackett, Wayne M Itano, Christopher Monroe, and David J Wineland. Experimental violation of a bell's inequality with efficient detection. *Nature*, 409(6822):791–794, 2001.

[82] Marissa Giustina, Alexandra Mech, Sven Ramelow, Bernhard Wittmann, Johannes Kofler, Jörn Beyer, Adriana Lita, Brice Calkins, Thomas Gerrits, Sae Woo Nam, et al. Bell violation using entangled photons without the fair-sampling assumption. *Nature*, 497(7448):227–230, 2013.

[83] Antony Eagle. Chance versus randomness. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, spring 2019 edition, 2019.

[84] Marissa Giustina, Marijn A. M. Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Morgan W. Mitchell, Jörn Beyer, Thomas Gerrits, Adriana E. Lita, Lynden K. Shalm, Sae Woo Nam, Thomas Scheidl, Rupert Ursin, Bernhard Wittmann, and Anton Zeilinger. Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons. *Phys. Rev. Lett.*, 115(25):250401, 2015.

[85] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, 2015.

[86] Lynden K. Shalm, Evan Meyer-Scott, Bradley G. Christensen, Peter Bierhorst, Michael A. Wayne, Martin J. Stevens, Thomas Gerrits, Scott Glancy, Deny R. Hamel, Michael S. Allman, Kevin J. Coakley, Shellee D. Dyer, Carson Hodge, Adriana E. Lita, Varun B. Verma, Camilla Lambrocco, Edward Tortorici, Alan L. Migdall, Yanbao Zhang, Daniel R. Kumor, William H. Farr, Francesco Marsili, Matthew D. Shaw, Jeffrey A. Stern, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Thomas Jennewein, Morgan W. Mitchell, Paul G. Kwiat, Joshua C. Bienfang, Richard P. Mirin, Emanuel Knill, and Sae Woo Nam. Strong Loophole-Free Test of Local Realism. *Phys. Rev. Lett.*, 115(25):250402, 2015.

[87] Dominik Rauch, Johannes Handsteiner, Armin Hochrainer, Jason Gallicchio, Andrew S Friedman, Calvin Leung, Bo Liu, Lukas Bulla, Sebastian Ecker, Fabian Steinlechner, et al. Cosmic bell test using random measurement settings from high-redshift quasars. *Physical review letters*, 121(8):080403, 2018.

[88] Časlav Brukner. On the quantum measurement problem. *arXiv:1507.05255*, 2015.

[89] Časlav Brukner. A No-Go Theorem for Observer-Independent Facts. *Entropy*, 20(5):350, 2018.

[90] Arthur Fine. Hidden variables, joint probability, and the bell inequalities. *Phys. Rev. Lett.*, 48:291–295, 1982.

[91] J. S. Bell and Alain Aspect. *Speakable and Unspeakable in Quantum Mechanics: Collected Papers on Quantum Philosophy*. Cambridge University Press, 2 edition, 2004.

[92] M. A. Broome, M. P. Almeida, A. Fedrizzi, and Andrew G. White. Reducing multi-photon rates in pulsed down-conversion by temporal multiplexing. *Optics Express*, 19(23):22698, 2011.

[93] Francesco Graffitti, Peter Barrow, Massimiliano Proietti, Dmytro Kundys, and Alessandro Fedrizzi. Independent high-purity photons created in domain-engineered crystals. *Optica*, 5(5):514–517, May 2018.

[94] Farid Shahandeh, Martin Ringbauer, Massimiliano Proietti, Fabio Costa, Austin P Lund, Francesco Graffitti, Peter Barrow, Alex Pickston, Dytro Kundys, Timothy C Ralph, and Alessandro Fedrizzi. Assisted macroscopic quantumness. *arXiv preprint arXiv:1711.10498*, 2017.

[95] R Healey. Pragmatist Quantum Realism. *Phil-Sci Archive: 14322*, 2018.

[96] Kok-Wei Bong, Aníbal Utreras-Alarcón, Farzad Ghafari, Yeong-Cherng Liang, Nora Tischler, Eric G Cavalcanti, Geoff J Pryde, and Howard M Wiseman. Testing the reality of wigner's friend's experience. *arXiv preprint arXiv:1907.05607*, 2019.

[97] Daniela Frauchiger and Renato Renner. Quantum theory cannot consistently describe the use of itself. *Nature communications*, 9(1):3711, 2018.

[98] Jan-Åke Larsson. Loopholes in Bell inequality tests of local realism. *J. Phys. A*, 47(42):424003, 2014.

[99] Marek Zukowski, Anton Zeilinger, Michael A Horne, and Aarthur K Ekert. "event-ready-detectors"bell experiment via entanglement swapping. *Physical Review Letters*, 71:4287–4290, 1993.

[100] J Calsamiglia and N. Lutkenhaus. Maximum efficiency of a linear-optical Bell-state analyzer. *Applied Physics B*, 72(1):67–71, 2001.

[101] Samuel L. Braunstein and A. Mann. Measurement of the Bell operator and quantum teleportation. *Physical Review A*, 51(3):R1727–R1730, 1995.

[102] John Archibald Wheeler and Richard Phillips Feynman. Interaction with the absorber as the mechanism of radiation. *Reviews of modern physics*, 17(2-3):157, 1945.

[103] John G Cramer. The transactional interpretation of quantum mechanics. *Reviews of Modern Physics*, 58(3):647, 1986.

[104] Carlo Rovelli. Relational quantum mechanics. *Int. J. Theor. Phys.*, 35(8):1637–1678, 1996.

[105] Christopher A Fuchs. Notwithstanding bohr, the reasons for qbism. *Mind and Matter*, 15(2):245–300, 2017.

[106] Asher Peres. Unperformed experiments have no results. *American Journal of Physics*, 46(7):745–747, 1978.

[107] Tim van Leent, Matthias Bock, Robert Garthoff, Kai Redeker, Wei Zhang, Tobias Bauer, Wenjamin Rosenfeld, Christoph Becher, and Harald Weinfurter. Long-distance distribution of atom-photon entanglement at telecom wavelength. *Physical Review Letters*, 124(1):010510, 2020.

[108] Wenjamin Rosenfeld, Daniel Burchardt, Robert Garthoff, Kai Redeker, Norbert Ortegel, Markus Rau, and Harald Weinfurter. Event-ready Bell test using entangled atoms simultaneously closing detection and locality loopholes. *Phys. Rev. Lett.*, 119(1):010402, 2017.

[109] Anna Tchebotareva, Sophie LN Hermans, Peter C Humphreys, Dirk Voigt, Peter J Harmsma, Lun K Cheng, Ad L Verlaan, Niels Dijkhuizen, Wim De Jong, Anaïs Dréau, et al. Entanglement between a diamond spin qubit and a photonic time-bin qubit at telecom wavelength. *Physical Review Letters*, 123(6):063601, 2019.

[110] CE Bradley, J Randall, MH Abobeih, RC Berrevoets, MJ Degen, MA Bakker, M Markham, DJ Twitchen, and TH Taminiau. A ten-qubit solid-state spin register with quantum memory up to one minute. *Physical Review X*, 9(3):031045, 2019.

[111] John-Mark A Allen, Jonathan Barrett, Dominic C Horsman, Ciarán M Lee, and Robert W Spekkens. Quantum common causes and quantum causal models. *Physical Review X*, 7(3):031021, 2017.

[112] Rafael Chaves, Daniel Cavalcanti, and Leandro Aolita. Causal hierarchy of multipartite bell nonlocality. *Quantum*, 1:23, 2017.

[113] Christopher J Wood and Robert W Spekkens. The lesson of causal discovery algorithms for quantum correlations: Causal explanations of bell-inequality violations require fine-tuning. *New Journal of Physics*, 17(3):033002, 2015.

[114] Stefano Pironio, Antonio Acin, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, 2009.

[115] Massimiliano Proietti, Joseph Ho, Federico Grasselli, Peter Barrow, Mehul Malik, and Alessandro Fedrizzi. Experimental quantum conference key agreement. *arXiv preprint arXiv:2002.01491*, 2020.

[116] Gilbert S Vernam. Cipher printing telegraph systems: For secret wire and radio telegraphic communications. *Journal of the AIEE*, 45(2):109–115, 1926.

[117] Claude E Shannon. Communication theory of secrecy systems. *Bell system technical journal*, 28(4):656–715, 1949.

[118] Gilles Brassard. Brief history of quantum cryptography: A personal perspective. In *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005.*, pages 19–23. IEEE, 2005.

[119] Charles H Bennett, Gilles Brassard, Seth Breidbart, and Stephen Wiesner. Quantum cryptography, or unforgeable subway tokens. In *Advances in Cryptology*, pages 267–275. Springer, 1983.

[120] Charles H Bennett and Gilles Brassard. Proceedings of the ieee international conference on computers, systems and signal processing, 1984.

[121] Artur K Ekert. Quantum cryptography based on bell's theorem. *Physical review letters*, 67(6):661, 1991.

[122] Renato Renner and Stefan Wolf. Simple and tight bounds for information reconciliation and privacy amplification. In *International conference on the*

theory and application of cryptology and information security, pages 199–216. Springer, 2005.

[123] Bruno Huttner, Nobuyuki Imoto, Nicolas Gisin, and Tsafrir Mor. Quantum cryptography with coherent states. *Physical Review A*, 51(3):1863, 1995.

[124] Norbert Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Physical Review A*, 61(5):052304, 2000.

[125] Won-Young Hwang. Quantum key distribution with high loss: toward global secure communication. *Physical Review Letters*, 91(5):057901, 2003.

[126] Xiang-Bin Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Physical Review Letters*, 94(23):230503, 2005.

[127] Xiang-Bin Wang. Decoy-state protocol for quantum cryptography with four different intensities of coherent light. *Physical Review A*, 72(1):012322, 2005.

[128] Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo. Practical decoy state for quantum key distribution. *Physical Review A*, 72(1):012326, 2005.

[129] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of modern physics*, 81(3):1301, 2009.

[130] Peter W Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical review letters*, 85(2):441, 2000.

[131] Claude Elwood Shannon. A mathematical theory of communication. *Bell system technical journal*, 27(3):379–423, 1948.

[132] Dagmar Bruß. Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, 81(14):3018, 1998.

[133] Charles H Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21):3121, 1992.

[134] William K Wootters and Wojciech H Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[135] Antonio Acin, Nicolas Gisin, and Lluis Masanes. From bell's theorem to secure quantum key distribution. *Physical Review Letters*, 97(12):120405, 2006.

[136] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98(23):230501, 2007.

[137] Charles H Bennett, Gilles Brassard, and N David Mermin. Quantum cryptography without bell's theorem. *Physical Review Letters*, 68(5):557, 1992.

[138] Gilles Brassard and Louis Salvail. Secret-key reconciliation by public discussion. *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 410–423, 1993.

[139] Robert Gallager. Low-density parity-check codes. *IRE Transactions on information theory*, 8(1):21–28, 1962.

[140] Mustafa Eroz, Feng-Wen Sun, and Lin-Nan Lee. Dvb-s2 low density parity check codes with near shannon limit performance. *International Journal of Satellite Communications and Networking*, 22(3):269–279, 2004.

[141] Alberto Morello and Vittoria Mignone. Dvb-s2: The second generation standard for satellite broad-band services. *Proceedings of the IEEE*, 94(1):210–227, 2006.

[142] Mario Milicevic, Chen Feng, Lei M Zhang, and P Glenn Gulak. Key reconciliation with low-density parity-check codes for long-distance quantum cryptography. *arXiv preprint arXiv:1702.07740*, 2017.

[143] David Elkouss, Anthony Leverrier, Romain Alléaume, and Joseph J Boutros. Efficient reconciliation protocol for discrete-variable quantum key distribution. *2009 IEEE International Symposium on Information Theory*, pages 1879–1883, 2009.

[144] David Elkouss, Jesus Martinez, Daniel Lancho, and Vicente Martin. Rate compatible protocol for information reconciliation: An application to qkd. In *2010 IEEE Information Theory Workshop on Information Theory (ITW 2010, Cairo)*, pages 1–5. IEEE, 2010.

[145] Paul Jouguet and Sebastien Kunz-Jacques. High performance error correction for quantum key distribution using polar codes. *arXiv preprint arXiv:1204.5882*, 2012.

[146] Kai Chen and Hoi-Kwong Lo. Conference key agreement and quantum sharing of classical secrets with noisy ghz states. *Proceedings of International Symposium on Information Theory*, pages 1607–1611, 2005.

[147] Momtchil Peev, Andreas Poppe, Oliver Maurhart, Thomas Lorünser, Thomas Länger, and Christoph Pacher. The SECOQC quantum key distribution network in Vienna. *European Conference on Optical Communication, ECOC*, 2009.

[148] Sören Wengerowsky, Siddarth Koduru Joshi, Fabian Steinlechner, Hannes Hübel, and Rupert Ursin. An entanglement-based wavelength-multiplexed quantum communication network. *Nature*, 564(7735):225–228, 2018.

[149] Federico Grasselli, Hermann Kampermann, and Dagmar Bruß. Finite-key effects in multipartite quantum key distribution protocols. *New Journal of Physics*, 20(11):113014, 2018.

[150] Michael Epping, Hermann Kampermann, Dagmar Bruß, et al. Multi-partite entanglement can speed up quantum key distribution in networks. *New Journal of Physics*, 19(9):093012, 2017.

[151] Robert M. Gray. Toeplitz and circulant matrices: A review. *Foundations and Trends in Communications and Information Theory*, 2(3):155–239, 2006.

[152] Niek J Bouman and Serge Fehr. Sampling in a quantum population, and applications. In *Annual Cryptology Conference*, pages 724–741. Springer, 2010.

[153] Matthew A Broome, Marcelo P Almeida, Alessandro Fedrizzi, and Andrew G White. Reducing multi-photon rates in pulsed down-conversion by temporal multiplexing. *Optics Express*, 19(23):22698–22708, 2011.

[154] Misha Brodsky, Elizabeth C George, Cristian Antonelli, and Mark Shtaif. Loss of polarization entanglement in a fiber-optic system with polarization mode dispersion in one optical path. *Optics letters*, 36(1):43–45, 2011.

[155] M. Hayashi. Exponential decreasing rate of leaked information in universal random privacy amplification. *IEEE Transactions on Information Theory*, 57(6):3989–4001, 2011.

[156] Timo Holz, Daniel Miller, Hermann Kampermann, and Dagmar Bruß. Comment on "fully device-independent conference key agreement". *Physical Review A*, 100:026301, 2019.

[157] Jérémy Ribeiro, Gláucia Murta, and Stephanie Wehner. Reply to "comment on 'fully device-independent conference key agreement'". *Physical Review A*, 100(2):026302, 2019.

[158] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nature communications*, 8:15043, 2017.

[159] Stefano Pirandola. End-to-end capacities of a quantum communication network. *Commun. Phys*, 2:51, 2019.

[160] Masahiro Takeoka, Eneet Kaur, Wojciech Roga, and Mark M Wilde. Multipartite entanglement and secret key distribution in quantum networks. *arXiv preprint arXiv:1912.10658*, 2019.

[161] Stefano Pirandola. General upper bounds for distributing conferencing keys in arbitrary quantum networks. *arXiv preprint arXiv:1912.11355*, 2019.

[162] Jérémy Ribeiro, Gláucia Murta, and Stephanie Wehner. Fully device-independent conference key agreement. *Physical Review A*, 97(2):022307, 2018.

[163] Matej Pivoluska, Marcus Huber, and Mehul Malik. Layered quantum key distribution. *Phys. Rev. A*, 97(3):032312, March 2018.

[164] Yonggi Jo and Wonmin Son. Semi-device-independent multiparty quantum key distribution in the asymptotic limit. *OSA Continuum*, 2(3):814–826, 2019.

[165] Michael Epping, Hermann Kampermann, and Dagmar Bruß. Robust entanglement distribution via quantum network coding. *New Journal of Physics*, 18(10), 2016.

[166] Karl Kraus, Arno Böhm, John D Dollard, and WH Wootters. States, effects, and operations fundamental notions of quantum theory. In *States, Effects, and Operations Fundamental Notions of Quantum Theory*, volume 190, 1983.

[167] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 10th edition, 2011.

[168] Maximilian A Schlosshauer. *Decoherence: and the quantum-to-classical transition*. Springer Science & Business Media, 2007.

[169] Wojciech Hubert Zurek. Decoherence, einselection, and the quantum origins of the classical. *Review of Modern Physics*, 75:715–775, 2003.

[170] Hans Aschauer and Hans J. Briegel. Quantum communication and decoherence. pages 235–261, 2002.

[171] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Advances in quantum metrology. *Nature Photonics*, 5(4):222, 2011.

[172] Michael Freedman, Alexei Kitaev, Michael Larsen, and Zhenghan Wang. Topological quantum computation. *Bulletin Am. Math. Soc.*, 40(1):31–38, 2003.

[173] Daniel A Lidar, Isaac L Chuang, and K Birgitta Whaley. Decoherence-free subspaces for quantum computation. *Physical Review Letters*, 81(12):2594, 1998.

[174] Yong Su Kim, Jong Chan Lee, Osung Kwon, and Yoon Ho Kim. Protecting entanglement from decoherence using weak measurement and quantum measurement reversal. *Nature Physics*, 8(2):117–120, 2012.

[175] Peter W. Shor. Scheme for reducing decoherence in quantum computer memory. *Physical Review A*, 52(4):2493–2496, 1995.

[176] A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098–1105, 1996.

[177] A. M. Steane. Error Correcting Codes in Quantum Theory. *Physical Review Letters*, 77(5):793–797, 1996.

[178] Daniel A Lidar and K Birgitta Whaley. Decoherence-free subspaces and subsystems. In *Irreversible quantum dynamics*, pages 83–120. Springer, 2003.

[179] Daniel A Lidar. Review of decoherence free subspaces, noiseless subsystems, and dynamical decoupling. *Adv. Chem. Phys*, 154:295–354, 2014.

[180] Dorit Aharonov and Michael Ben-Or. Fault-Tolerant Quantum Computation with Constant Error Rate. *SIAM J. Comp.*, 38(4):1207–1282, 2008.

[181] Rafael Chaves, Leandro Aolita, and Antonio Acín. Robust multipartite quantum correlations without complex encodings. *Physical Review A*, 86(2):020301, 2012.

[182] Massimiliano Proietti, Martin Ringbauer, Francesco Graffitti, Peter Barrow, Alexander Pickston, Dmytro Kundys, Daniel Cavalcanti, Leandro Aolita, Rafael Chaves, and Alessandro Fedrizzi. Enhanced multiqubit phase estimation in noisy environments by local encoding. *Physical Review Letters*, 123(18):180503, 2019.

[183] Daniel M. Greenberger, Michael A. Horne, Abner Shimony, and Anton Zeilinger. Bell's theorem without inequalities. *Am. J. Phys.*, 58(12):1131, 1990.

[184] L. Aolita, R. Chaves, D. Cavalcanti, A. Acín, and L. Davidovich. Scaling laws for the decay of multiqubit entanglement. *Physical Review Letters*, 100:080501, Feb 2008.

[185] L. Aolita, F de Melo, and L. Davidovich. Open-system dynamics of entanglement:a key issues review. *Rep. Prog. Phys.*, 78:042001, 2015.

[186] Joseph M. Renes, Robin Blume-Kohout, A. J. Scott, and Carlton M. Caves. Symmetric informationally complete quantum measurements. *J. Math. Phys.*, 45(6):2171–2180, 2004.

[187] Alexander Streltsov, Gerardo Adesso, and Martin B. Plenio. Colloquium : Quantum coherence as a resource. *Review of Modern Physics*, 89(4):041003, 2017.

[188] Carmine Napoli, Thomas R. Bromley, Marco Cianciaruso, Marco Piani, Nathaniel Johnston, and Gerardo Adesso. Robustness of Coherence: An Operational and Observable Measure of Quantum Coherence. *Physical Review Letters*, 116(15):150502, 2016.

[189] Martin Ringbauer, Thomas R. Bromley, Marco Cianciaruso, Ludovico Lami, W. Y. Sarah Lau, Gerardo Adesso, Andrew G. White, Alessandro Fedrizzi, and Marco Piani. Certification and quantification of multilevel quantum coherence. *Physical Review X*, 8:041007, Oct 2018.

[190] Chao Zhang, Thomas R Bromley, Yun-Feng Huang, Huan Cao, Wei-Min Lv, Bi-Heng Liu, Chuan-Feng Li, Guang-Can Guo, Marco Cianciaruso, and Gerardo Adesso. Demonstrating resilient quantum coherence and metrology to transversal noise. *arXiv preprint arXiv:1907.10540*, 2019.

[191] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum-enhanced measurements: beating the standard quantum limit. *Science*, 306(5700):1330–1336, 2004.

[192] G. Tóth and I. Apellaniz. Quantum metrology from a quantum information science perspective. *Journal of Physics A*, 47:424006, 2014.

[193] Ronald Aylmer Fisher. Statistical methods for research workers. In *Breakthroughs in statistics*, pages 66–70. Springer, 1992.

[194] Alexander S Holevo. Probabilistic and statistical aspects of quantum theory. 1, 2011.

[195] Harald Cramér. *Mathematical methods of statistics*, volume 43. Princeton university press, 1999.

[196] C Radhakrishna Rao. Information and the accuracy attainable in the estimation of statistical parameters. In *Breakthroughs in statistics*, pages 235–247. Springer, 1992.

[197] Carl W Helstrom. Quantum detection and estimation theory. *J. Stat. Phys.*, 1(2):231–252, 1969.

[198] Rafal Demkowicz-Dobrzański and Lorenzo Maccone. Using entanglement against noise in quantum metrology. *Physical Review Letters*, 113(25):250801, 2014.

[199] Stefano Pirandola and Cosmo Lupo. Ultimate precision of adaptive noise estimation. *Physical Review Letters*, 118:100502, 2017.

[200] Géza Tóth. Multipartite entanglement and high-precision metrology. *Physical Review A*, 85:022322, 2012.

[201] Philipp Hyllus, Wiesław Laskowski, Roland Krischek, Christian Schwemmer, Witlef Wieczorek, Harald Weinfurter, Luca Pezzé, and Augusto Smerzi. Fisher information and multiparticle entanglement. *Physical Review A*, 85:022321, 2012.

[202] Samuel L. Braunstein and Carlton M. Caves. Statistical distance and the geometry of quantum states. *Physical Review Letters*, 72:3439–3443, 1994.

[203] Jing Liu, Xiao-Xing Jing, Wei Zhong, and Xiao-Guang Wang. Quantum Fisher Information for Density Matrices with Arbitrary Ranks. *Commun. Theor. Phys.*, 61(1):45–50, 2014.

[204] R. Chaves, J. B. Brask, M. Markiewicz, J. Kołodyński, and A. Acín. Noisy metrology beyond the standard quantum limit. *Physical Review Letters*, 111:120401, 2013.

[205] Francesco Graffitti, Peter Barrow, Massimiliano Proietti, Dmytro Kundys, and Alessandro Fedrizzi. Independent high-purity photons created in domain-engineered crystals. *Optica*, 5(5):514–517, 2018.

[206] Chong-Ki Hong, Zhe-Yu Ou, and Leonard Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.*, 59(18):2044, 1987.

[207] Erich Joos, H. Dieter Zeh, Claus Kiefer, Domenico Giulini, Joachim Kupsch, and Ion-Olimpiu Stamatescu. *Decoherence and the Appearance of a Classical World in Quantum Theory*. Springer, Heidelberg, 2003.

[208] Wojciech Hubert Zurek. Decoherence, einselection, and the quantum origins of the classical. *Review of Modern Physics*, 75(3):715–775, 2003.

[209] Sadegh Raeisi, Pavel Sekatski, and Christoph Simon. Coarse Graining Makes It Hard to See Micro-Macro Entanglement. *Physical Review Letters*, 107(25):250401, 2011.

[210] Chang-Woo Lee and Hyunseok Jeong. Quantification of Macroscopic Quantum Superpositions within Phase Space. *Physical Review Letter*, 106(22):220401, 2011.

[211] F. Fröwis and W. Dür. Are Cloned Quantum States Macroscopic? *Physical Review Letters*, 109(17):170401, 2012.

[212] Pavel Sekatski, Nicolas Gisin, and Nicolas Sangouard. How Difficult Is It to Prove the Quantumness of Macroscropic States? *Physical Review Letters*, 113(9):090403, 2014.

[213] Pavel Sekatski, Nicolas Sangouard, and Nicolas Gisin. Size of quantum superpositions as measured with classical detectors. *Physical Review A*, 89(1):012116, 2014.

[214] Amine Laghaout, Jonas S. Neergaard-Nielsen, and Ulrik L. Andersen. Assessments of macroscopicity for quantum optical states. *Optical Communications*, 337:96–101, 2014.

[215] Tristan Farrow and Vlatko Vedral. Classification of macroscopic quantum effects. *Opt. Commun.*, 337:22–26, 2015.